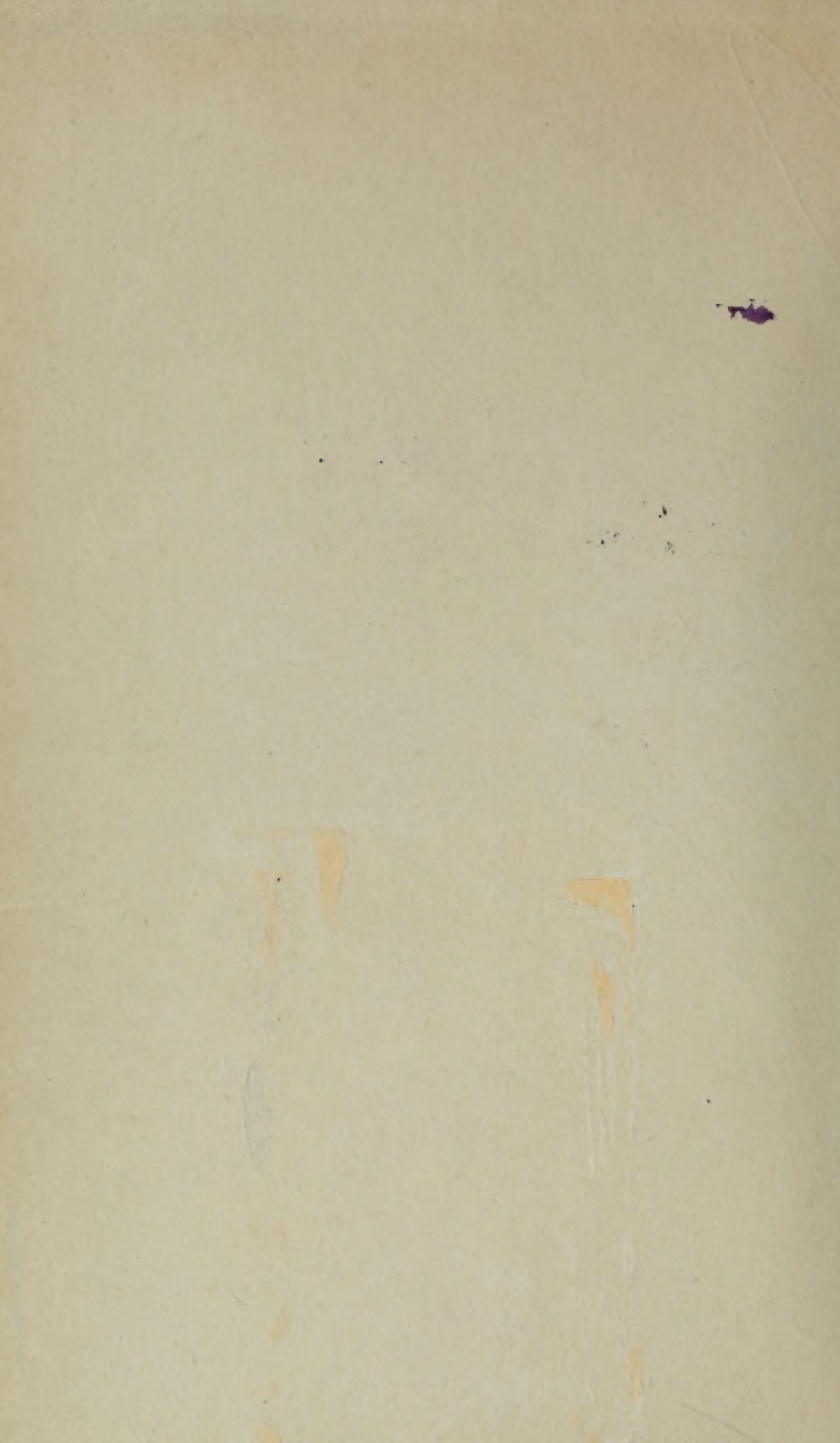


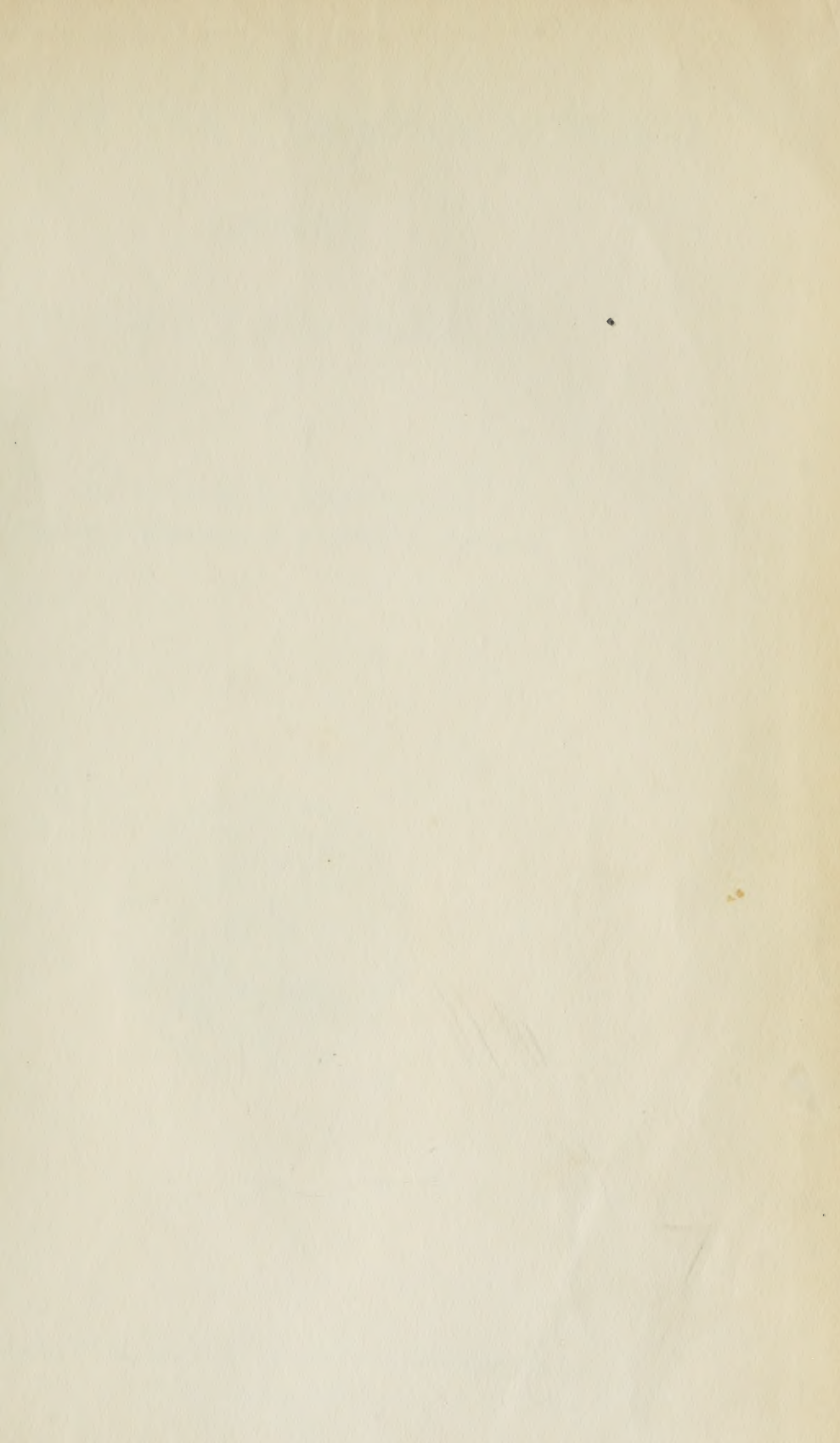
University of
Southern R
Library R



This book is DUE on last date stamped below

MAR 2 1963

SOUTHERN BRANCH,
UNIVERSITY OF CALIFORNIA,
LIBRARY,
LOS ANGELES, CALIF.



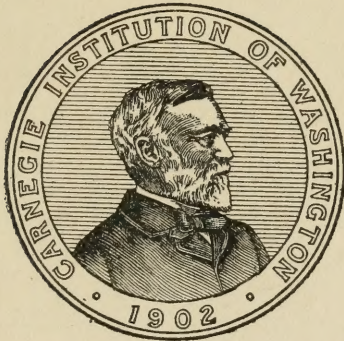
HISTORY OF THE THEORY OF NUMBERS

VOLUME I

DIVISIBILITY AND PRIMALITY

BY LEONARD EUGENE DICKSON

Professor of Mathematics in the University of Chicago



PUBLISHED BY THE CARNEGIE INSTITUTION OF WASHINGTON

WASHINGTON, 1919

71785

CARNEGIE INSTITUTION OF WASHINGTON

PUBLICATION No. 256, Vol. I

ANNUAL REPORT
FOR THE YEAR
1908

PRESS OF GIBSON BROTHERS
WASHINGTON, D. C.

QA
241
D56h
v.1
cop. 2

Engineering &
Mathematical
Sciences
Library

PREFACE.

The efforts of Cantor and his collaborators show that a chronological history of mathematics down to the nineteenth century can be written in four large volumes. To cover the last century with the same elaborateness, it has been estimated that about fifteen volumes would be required, so extensive is the mathematical literature of that period. But to retain the chronological order and hence devote a large volume to a period of at most seven years would defeat some of the chief purposes of a history, besides making it very inconvenient to find all of the material on a particular topic. In any event there is certainly need of histories which treat of particular branches of mathematics up to the present time.

The theory of numbers is especially entitled to a separate history on account of the great interest which has been taken in it continuously through the centuries from the time of Pythagoras, an interest shared on the one extreme by nearly every noted mathematician and on the other extreme by numerous amateurs attracted by no other part of mathematics. This history aims to give an adequate account of the entire literature of the theory of numbers. The first volume presents in twenty chapters the material relating to divisibility and primality. The concepts, results, and authors cited are so numerous that it seems appropriate to present here an introduction which gives for certain chapters an account in untechnical language of the main results in their historical setting, and for the remaining chapters the few remarks sufficient to clearly characterize the nature of their contents.

Perfect numbers have engaged the attention of arithmeticians of every century of the Christian era. It was while investigating them that Fermat discovered the theorem which bears his name and which forms the basis of a large part of the theory of numbers. A perfect number is one, like $6 = 1 + 2 + 3$, which equals the sum of its divisors other than itself. Euclid proved that $2^{p-1}(2^p - 1)$ is a perfect number if $2^p - 1$ is a prime. For $p = 2, 3, 5, 7$, the values 3, 7, 31, 127 of $2^p - 1$ are primes, so that 6, 28, 496, 8128 are perfect numbers, as noted by Nicomachus (about A. D. 100). A manuscript dated 1456 correctly gave 33550336 as the fifth perfect number; it corresponds to the value 13 of p . Very many early writers believed that $2^p - 1$ is a prime for every odd value of p . But in 1536 Regius noted that

$$2^9 - 1 = 511 = 7 \cdot 73, \quad 2^{11} - 1 = 2047 = 23 \cdot 89$$

are not primes and gave the above fifth perfect number. Cataldi, who founded at Bologna the most ancient known academy of mathematics,

noted in 1603 that $2^p - 1$ is composite if p is composite and verified that it is a prime for $p = 13, 17$, and 19 ; but he erred in stating that it is also a prime for $p = 23, 29$, and 37 . In fact, Fermat noted in 1640 that $2^{23} - 1$ has the factor 47 , and $2^{37} - 1$ the factor 223 , while Euler observed in 1732 that $2^{29} - 1$ has the factor 1103 . Of historical importance is the statement made by Mersenne in 1644 that the first eleven perfect numbers are given by $2^{p-1}(2^p - 1)$ for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$; but he erred at least in including 67 and excluding $61, 89$, and 107 . That $2^{67} - 1$ is composite was proved by Lucas in 1876, while its actual factors were found by Cole in 1903. The primality of $2^{61} - 1$, a number of 19 digits, was established by Pervušin in 1883, Seelhoff in 1886, and Hudelot in 1887. Both Powers and Fauquembergue proved in 1911-14 that $2^{89} - 1$ and $2^{107} - 1$ are primes. The primality of $2^{31} - 1$ and $2^{127} - 1$ had been established by Euler and Lucas respectively. Thus $2^p - 1$ is known to be a prime, and hence lead to a perfect number, for the twelve values $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ and 127 of p . Since $2^p - 1$ is known (pp. 15-31) to be composite for 32 primes $p \leq 257$, only the eleven values $p = 137, 139, 149, 157, 167, 193, 199, 227, 229, 241, 257$ now remain in doubt.

Descartes stated in 1638 that he could prove that every even perfect number is of Euclid's type and that every odd perfect number must be of the form ps^2 , where p is a prime. Euler's proofs (p. 19) were published after his death. An immediate proof of the former fact was given by Dickson (p. 30). According to Sylvester (pp. 26-27), there exists no odd perfect number with fewer than six distinct prime factors, and none with fewer than eight if not divisible by 3. But the question of the existence of odd perfect numbers remains unanswered.

A multiply perfect number, like 120 and 672 , is one the sum of whose divisors equals a multiple of the number. They were actively investigated during the years 1631-1647 by Mersenne, Fermat, St. Croix, Frenicle, and Descartes. Many new examples have been found recently by American writers.

Two numbers are called amicable if each equals the sum of the aliquot divisors of the other, where an aliquot divisor of a number means a divisor other than the number itself. The pair 220 and 284 was known to the Pythagoreans. In the ninth century, the Arab Thâbit ben Korrah noted that 2^nh and 2^ns are amicable numbers if $h = 3 \cdot 2^n - 1$, $t = 3 \cdot 2^{n-1} - 1$ and $s = 9 \cdot 2^{2n-1} - 1$ are all primes, and $n > 1$. This result leads to amicable numbers for $n = 2$ (giving the above pair), $n = 4$ and $n = 7$, but for no further value ≤ 200 of n . The chief investigation of amicable numbers is that by Euler who listed (pp. 45, 46) 62 pairs. At the age of 16, Paganini announced in 1866 the remarkable new pair 1184 and 1210 . A few new pairs of very large numbers have been found by Legendre, Seelhoff, and Dickson.

Interesting amicable triples and amicable numbers of higher order have been recently found by Dickson and Poulet (p. 50).

Although it had been employed in the study of perfect and amicable numbers, the explicit expression for the sum $\sigma(n)$ of all the divisors of n is reserved for Chapter II, in which is presented the history of Fermat's two problems to solve $\sigma(x^3)=y^2$ and $\sigma(x^2)=y^3$ and John Wallis's problem to find solutions other than $x=4$ and $y=5$ of $\sigma(x^2)=\sigma(y^2)$.

Fermat stated in 1640 that he had a proof of the fact, now known as Fermat's theorem, that, if p is any prime and x is any integer not divisible by p , then $x^{p-1}-1$ is divisible by p . This is one of the fundamental theorems of the theory of numbers. The case $x=2$ was known to the Chinese as early as 500 B. C. The first published proof was given by Euler in 1736. Of first importance is the generalization from the case of a prime p to any integer n , published by Euler in 1760: if $\phi(n)$ denotes the number of positive integers not exceeding n and relatively prime to n , then $x^{\phi(n)}-1$ is divisible by n for every integer x relatively prime to n . Another elegant theorem states that, if p is a prime, $1+\{1\cdot2\cdot3\cdots(p-1)\}$ is divisible by p ; it was first published by Waring in 1770, who ascribed it to Sir John Wilson. This theorem was stated at an earlier date in a manuscript by Leibniz, who with Newton discovered the calculus. But Lagrange was the first one to publish (in 1773) a proof of Wilson's theorem and to observe that its converse is true. In 1801 Gauss stated and suggested methods to prove the generalization of Wilson's theorem: if P denotes the product of the positive integers less than A and prime to A , then $P+1$ is divisible by A if $A=4$, p^m or $2p^m$, where p is an odd prime, while $P-1$ is divisible by A if A is not of one of these three forms. A very large number of proofs of the preceding theorems are given in the first part of Chapter III. Various generalizations are then presented (pp. 84-91). For instance, if $N=p_1^{e_1}\cdots p_s^{e_s}$, where p_1, \dots, p_s are distinct primes,

$$a^N - (a^{N/p_1} + \dots + a^{N/p_s}) + (a^{N/p_1 p_2} + \dots) - \dots + (-1)^s a^{N/p_1 \dots p_s}$$

is divisible by N , a fact due to Gauss for the case in which a is a prime.

Many cases have been found in which $a^{n-1}-1$ is divisible by n for a composite number n . But Lucas proved the following converse of Fermat's theorem: if a^x-1 is divisible by n when $x=n-1$, but not when x is a divisor $< n-1$ of $n-1$, then n is a prime.

Any integral symmetric function of degree d of $1, 2, \dots, p-1$ with integral coefficients is divisible by the prime p if d is not a multiple of $p-1$. A generalization to the case of a divisor p^n is due to Meyer (p. 101). Nielsen proved in 1893 that, if p is an odd prime and if k is odd and $1 < k < p-1$, the sum of the products of $1, 2, \dots, p-1$ taken k at a time is divisible by p^2 . Taking $k=p-2$, we see that if p is a prime > 3 the numerator of the fraction

equal to $1 + 1/2 + 1/3 + \dots + 1/(p-1)$ is divisible by p^2 , a result first proved by Wolstenholme in 1862. Sylvester stated in 1866 that the sum of all products of n distinct numbers chosen from $1, 2, \dots, m$ is divisible by each prime $> n+1$ which is contained in any term of the set $m-n+1, \dots, m, m+1$. There are various theorems analogous to these.

In Chapter IV are given properties of the quotient $(u^{p-1}-1)/p$, which plays an important rôle in recent investigations on Fermat's last theorem (the impossibility of $x^p + y^p = z^p$ if $p > 2$), the history of which will be treated in the final chapter of Volume II. Some of the present papers relate to $(u^{\phi(n)}-1)/n$, where n is not necessarily a prime.

While Euler's ϕ -function was defined above in order to state his generalization of Fermat's theorem, its numerous properties and generalizations are reserved for the long Chapter V. In 1801 Gauss gave the result that $\phi(d_1) + \dots + \phi(d_k) = n$, if d_1, \dots, d_k are the divisors of n ; this was generalized by Laguerre in 1872, H. G. Cantor in 1880, Busche in 1888, Zsigmondy in 1893, Vahlen in 1895, Elliott in 1901, and Hammond in 1916. In 1808 Legendre proved a simple formula for the number of integers $\leq n$ which are divisible by no one of any given set of primes. The asymptotic value of $\phi(1) + \dots + \phi(G)$ for G large was discussed by Dirichlet in 1849, Mertens in 1874, Perott in 1881, Sylvester in 1883 and 1897, Cesàro in 1883 and 1886-8, Berger in 1891, and Kronecker in 1901. The solution of $\phi(x) = g$ was treated by Cayley in 1857, Minin in 1897, Pichler in 1900, Carmichael in 1907-9, Ranum in 1908, and Cunningham in 1915. H. J. S. Smith proved in 1875 that the m -rowed determinant, having as the element in the i th row and j th column any function $f(\delta)$ of the greatest common divisor δ of i and j , equals the product of $F(1), F(2), \dots, F(m)$, where

$$F(m) = f(m) - \Sigma f\left(\frac{m}{p}\right) + \Sigma f\left(\frac{m}{pq}\right) - \dots, \quad m = p^a q^b \dots$$

In particular, $F(m) = \phi(m)$ if $f(\delta) = \delta$. In several papers (pp. 128-130) Cesàro considered analogous determinants. The fact that 30 is the largest number such that all smaller numbers relatively prime to it are primes was first proved by Schatunowsky in 1893.

A. Thacker in 1850 evaluated the sum $\phi_k(n)$ of the k th powers of the integers $\leq n$ which are prime to n . His formula has been expressed in various symbolic forms by Cesàro and generalized by Glaisher and Nielsen. Crelle had noted in 1845 that $\phi_1(n) = \frac{1}{2}n\phi(n)$. In 1869 Schemmel considered the number of sets of n consecutive integers each $< m$ and prime to m . In connection with linear congruence groups, Jordan evaluated the number of different sets of k positive integers $\leq n$ whose greatest common divisor is prime to n . This generalization of Euler's ϕ -function has properties as simple as the latter function and occurs in many papers under a variety of notations. It in turn has been generalized (pp. 151-4).

The properties of the set of all irreducible fractions, arranged in order of magnitude, whose numerators are $\leq m$ and denominators are $\leq n$ (called a Farey series if $m=n$), have been discussed by many writers and applied to the approximation of numbers, to binary quadratic forms, to the composition of linear fractional substitutions, and to geometry (pp. 155-8).

Some of the properties of periodic decimal fractions are already familiar to the reader in view of his study of arithmetic and the chapter of algebra dealing with the sum to infinity of a geometric progression. For the generalization to periodic fractions to any base b , not necessarily 10, the length of the period of the periodic fraction for $1/d$, where d is prime to b , is the least positive exponent e such that $b^e - 1$ is divisible by d . Hence this Chapter VI, which reports upon more than 160 papers, is closely related to the following chapter and furnishes a concrete introduction to it.

The subject of exponents and primitive roots is one of the important topics of the theory of numbers. To present the definitions in the customary, compact language, we shall need the notion of congruence. If the difference of two integers a and b is divisible by m , they are called congruent modulo m and we write $a \equiv b \pmod{m}$. For example, $8 \equiv 2 \pmod{6}$. If $n^e \equiv 1 \pmod{m}$, but $n^s \not\equiv 1 \pmod{m}$ for $0 < s < e$, we say that n belongs to the exponent e modulo m . For example, 2 and 3 belong to the exponent 4 modulo 5, while 4 belongs to the exponent 2. In view of Euler's generalization of Fermat's theorem, stated above, e never exceeds $\phi(m)$. If n belongs to this maximum exponent $\phi(n)$ modulo m , n is called a primitive root of m . For example, 2 and 3 are primitive roots of 5, while 1 and 4 are not. Lambert stated in 1769 that there exists a primitive root of any prime p , and Euler gave a defective proof in 1773. In 1785 Legendre proved that there are exactly $\phi(e)$ numbers belonging modulo p to any exponent e which divides $p-1$. In 1801 Gauss proved that there exist primitive roots of m if and only if $m=2, 4, p^k$ or $2p^k$, where p is an odd prime. In particular, for a primitive root a of a prime modulus p and any integer N not divisible by p , there is an exponent $\text{ind } N$, called the index of N by Gauss, such that $N \equiv a^{\text{ind } N} \pmod{p}$. Indices play a rôle similar to logarithms, but we require two companion tables for each modulus p . The extension to a power of prime modulus is immediate. For a general modulus, systems of indices were employed by Dirichlet in 1837 and 1863 and by Kronecker in 1870. Jacobi's Canon Arithmeticus of 1839 gives companion tables of indices for each prime and power of a prime < 1000 . Cunningham's Binary Canon of 1900 gives the residues of the successive powers of 2 when divided by each prime or power of a prime < 1000 and companion tables showing the powers of 2 whose residues are 1, 2, 3, In 1846 Arndt proved that, if g is a primitive root of the odd prime p , g belongs to the exponent $p^{n-\lambda}(p-1)$ modulo p^n if and only if $G = g^{p-1} - 1$ is divisible by p^λ , but not by $p^{\lambda+1}$, where

$\lambda < n$; taking $\lambda = 1$, we see that, if G is not divisible by p^2 , g is a primitive root of p^2 and of all higher powers of p . This Chapter VII presents many more theorems on exponents, primitive roots, and binomial congruences, and cites various lists of primitive roots of primes < 10000 .

Lagrange proved easily that a congruence of degree n has at most n roots if the modulus is a prime. Lebesgue found the number of sets of solutions of $a_1x_1^m + \dots + a_kx_k^m \equiv a \pmod{p}$, when p is a prime such that $p-1$ is divisible by m . König (p. 226) employed a cyclic determinant and its minors to find the exact number of real roots of any congruence in one unknown; Gegenbauer (p. 228) and Rados (p. 233) gave generalizations to congruences in several unknowns.

Galois's introduction of imaginary roots of congruences has not only led to an important extension of the theory of numbers, but has given rise to wide generalizations of theorems which had been obtained in subjects like linear congruence groups by applying the ordinary theory of numbers. Instead of the residues of integers modulo p , let us consider the residues of polynomials in a variable x with integral coefficients with respect to two moduli, one being a prime p and the other a polynomial $f(x)$ of degree n which is irreducible modulo p . The residues are the p^n polynomials in x of degree $n-1$ whose coefficients are chosen from the set $0, 1, \dots, p-1$. These residues form a Galois field within which can be performed addition, subtraction, multiplication, and division (except by zero). As a generalization of Fermat's theorem, Galois proved that the power $p^n - 1$ of any residue except zero is congruent to unity with respect to our pair of moduli p and $f(x)$. He avoided our second modulus $f(x)$ by introducing an undefined imaginary root i of $f(x) \equiv 0 \pmod{p}$ and considering the residues modulo p of polynomials in i ; but the above use of the two moduli affords the only logical basis of the theory. In view of the fullness of the reports in the text (pp. 233-252) of the papers on this subject, further comments here are unnecessary. The final topics of this long Chapter VIII are cubic congruences and miscellaneous results on congruences and possess little general interest.

In Chapter IX are given Legendre's expression for the exponent of the highest power of a prime p which divides the factorial $1 \cdot 2 \cdot \dots \cdot m$, and the generalization to the product of any integers in arithmetical progression; many theorems on the divisibility of one product of factorials by another product and on the residues of multinomial coefficients; various determinations of the sign in $1 \cdot 2 \cdot \dots \cdot (p-1)/2 \equiv \pm 1 \pmod{p}$; and miscellaneous congruences involving factorials.

In the extensive Chapter X are given many theorems and formulas concerning the sum of the k th powers of all the divisors of n , or of its even or odd divisors, or of its divisors which are exact s th powers, or of those divisors

whose complementary divisors are even or odd or are exact sth powers, and the excess of the sum of the k th powers of the divisors of the form $4m+1$ of a number over the sum of the k th powers of the divisors of the form $4m+3$, as well as more technical sums of divisors defined on pages 297, 301-2, 305, 307-8, 314-5 and 318. For the important case $k=0$, such a sum becomes the number of the divisors in question. There are theorems on the number of sets of positive integral solutions of $u_1u_2\dots u_k=n$ or of $x^ay^b=n$. Also Glaisher's cancellation theorems on the actual divisors of numbers (pp. 310-11, 320-21). Scattered through the chapter are approximation and asymptotic formulas involving some of the above functions.

In Chapter XI occur Dirichlet's theorem on the number of cases in the division of n by $1, 2, \dots, p$ in turn in which the ratio of the remainder to the divisor is less than a given proper fraction, and the generalizations on pp. 330-1; theorems on the number of integers $\leq n$ which are divisible by no exact sth power >1 ; theorems on the greatest divisor which is odd or has specified properties; many theorems on greatest common divisor and least common multiple; and various theorems on mean values and probability.

The casting out of nines or of multiples of 11 or 7 to check arithmetical computations is of early origin. This topic and the related one of testing the divisibility of one number by another have given rise to the numerous elementary papers cited in Chapter XII.

The frequent need of the factors of numbers and the excessive labor required for their direct determination have combined to inspire the construction of factor tables of continually increasing limit. The usual method is essentially that given by Eratosthenes in the third century B. C. A special method is used by Lebon (pp. 355-6). Attention is called to Lehmer's Factor Table for the First Ten Millions and his List of Prime Numbers from 1 to 10,006,721, published in 1909 and 1914 by the Carnegie Institution of Washington. Since these tables were constructed anew with the greatest care and all variations from the chief former tables were taken account of, they are certainly the most accurate tables extant. Absolute accuracy is here more essential than in ordinary tables of continuous functions. Besides giving the history of factor tables and lists of primes, this Chapter XIII cites papers which enumerate the primes in various intervals, prime pairs (as 11, 13), primes of the form $4n+1$, and papers listing primes written to be base 2 or large primes.

Chapter XIV cites the papers on factoring a number by expressing it as a difference of two squares, or as a sum of two squares in two ways, or by use of binary quadratic forms, the final digits, continued fractions, Pell equations, various small moduli, or miscellaneous methods.

Fermat expressed his belief that $F_n = 2^{2^n} + 1$ is a prime for every value of n . While this is true if $n = 1, 2, 3, 4$, it fails for $n = 5$ as noted by Euler. Later,

Gauss proved that a regular polygon of m sides can be constructed by ruler and compasses if m is a product of a power of 2 and distinct odd primes each of the form F_n , and stated correctly that the construction is impossible if m is not such a product. In view of the papers cited in Chapter XV, F_n is composite if $n = 5, 6, 7, 8, 9, 11, 12, 18, 23, 36, 38$ and 73, while nothing is known for other values > 4 of n . No comment will be made on the next chapter which treats of the factors of numbers of the form $a^n \pm b^n$ and of certain trinomials.

In Chapter XVII are treated questions on the divisors of terms of a recurring series and in particular of Lucas' functions

$$u_n = \frac{a^n - b^n}{a - b}, \quad v_n = a^n + b^n,$$

where a and b are roots of $x^2 - Px + Q = 0$, P and Q being relatively prime integers. By use of these functions, Lucas obtained an extension of Euler's generalization of Fermat's theorem, which requires the correction noted by Carmichael (p. 406), as well as various tests for primality, some of which have been employed in investigations on perfect numbers. Many papers on the algebraic theory of recurring series are cited at the end of the chapter.

Euclid gave a simple and elegant proof that the number of primes is infinite. For the generalization that every arithmetical progression $n, n+m, n+2m, \dots$, in which n and m are relatively prime, contains an infinitude of primes, Legendre offered an insufficient proof, while Dirichlet gave his classic proof by means of infinite series and the classes of binary quadratic forms, and extended the theorem to complex integers. Mertens and others obtained simpler proofs. For various special arithmetical progressions, the theorem has been proved in elementary ways by many writers. Dirichlet also obtained the theorems that, if $a, 2b$, and c have no common factor, $ax^2 + 2bxy + cy^2$ represents an infinitude of primes, while an infinitude of these primes are representable by any given linear form $Mx + N$ with M and N relatively prime, provided a, b, c, M, N are such that the quadratic and linear forms can represent the same number.

No complete proof has been found for Goldbach's conjecture in 1742 that every even integer is a sum of two primes. One of various analogous unproved conjectures is that every even integer is the difference of two consecutive primes in an infinitude of ways (in particular, there exists an infinitude of pairs of primes differing by 2). No comment will be made on the further topics of this Chapter XVIII: polynomials representing numerous primes, primes in arithmetical progression, tests for primality, number of primes between assigned limits, Bertrand's postulate of the existence of at least one prime between x and $2x-2$ for $x > 3$, miscellaneous results on primes, diatomic series, and asymptotic distribution of primes.

If $F(m) = \sum f(d)$, summed for all the divisors d of m , we can express $f(m)$ in terms of F by an inversion formula given in Chapter XIX along with generalizations and related formulas. Bougaief called $F(m)$ the numerical integral of $f(m)$.

The final Chapter XX gives many elementary results involving the digits of numbers mainly when written to the base 10.

Since the history of each main topic is given separately, it has been possible without causing confusion to include reports on minor papers and isolated problems for the sake of completeness. In the cases of books and journals not usually accessible, the reports are quite full with some indication of the proofs. In other cases, proofs are given only when necessary to differentiate the paper from others deriving the same result.

The references were selected mainly from the Subject Index of the Royal Society of London Catalogue of Scientific Papers, volume I, 1908 (with which also the proof-sheets were checked), and the supplementary annual volumes forming the International Catalogue of Scientific Literature, *Jahrbuch über die Fortschritte der Mathematik*, *Revue semestrielle des publications mathématiques*, Poggendorff's *Handwörterbuch*, Klügel's *Mathematische Wörterbuch*, Wölffing's *Mathematischer Bücherschatz* (a list of mathematical books and pamphlets of the nineteenth century), historical journals, such as *Bulletino di bibliografia e di storia delle scienze matematiche e fisiche*, *Bolletino* . . . , *Bibliotheca Mathematica*, *Abhandlungen zur Geschichte der mathematischen Wissenschaften*, various histories and encyclopedias, including the *Encyclopédie des sciences mathématiques*. Further, the author made a direct examination at the stacks of books and old journals in the libraries of Chicago, California, and Cambridge Universities, and Trinity College, Cambridge, and the excellent John Crerar Library at Chicago. He made use of G. A. Plimpton's remarkable collection, in New York, of rare books and manuscripts. In 1912 the author made an extended investigation in the libraries of the British Museum, Kensington Museum, Royal Society, Cambridge Philosophical Society, *Bibliothèque Nationale*, *Université de Paris*, *St. Geneviève*, *l'Institut de France*, *University of Göttingen*, and the *Königliche Bibliothek of Berlin* (where there is a separate index of the material on the theory of numbers). Many books have since been borrowed from various libraries; the Ladies' and other Diaries were loaned by R. C. Archibald.

At the end of the volume is a separate index of authors for each of the twenty chapters, which will facilitate the tracing of the relation of a paper to kindred papers and hence will be of special service in the case of papers inaccessible to the reader. The concluding volume will have a combined index of authors from which will be omitted minor citations found in the chapter indices.

The subject index contains a list of symbols; while $[x]$ usually denotes the greatest integer $\leq x$, occasionally such square brackets are used to inclose an addition to a quotation. The symbol * before an author's name signifies that his paper was not available for report. The symbol † before a date signifies date of death. Initials are given only in the first of several immediately successive citations of an author.

Although those volumes of Euler's Opera Omnia which contain his Commentationes Arithmeticae Collectae have been printed, they are not yet available; a table showing the pages of the Opera and the corresponding pages in the present volume of this history will be given in the concluding volume.

The author is under great obligations to the following experts in the theory of numbers for numerous improvements resulting from their reading the initial page proofs of this volume: R. D. Carmichael, L. Chanzy, A. Cunningham, E. B. Escott, A. Gérardin, A. J. Kempner, D. N. Lehmer, E. Maillet, L. S. Shively, and H. J. Woodall; also the benefit of D. E. Smith's accurate and extensive acquaintance with early books and writers was fortunately secured; and the author's special thanks are due to Carmichael and Kempner, who read the final page proofs with the same critical attention as the initial page proofs and pointed out various errors and obscurities. To these eleven men who gave so generously of their time to perfect this volume, and especially to the last two, is due the gratitude of every devotee of number theory who may derive benefit or pleasure from this history. In return, such readers are requested to further increase the usefulness of this work by sending corrections, notices of omissions, and abstracts of papers marked not available for report, for insertion in the concluding volume.

Finally, this laborious project would doubtless have been abandoned soon after its inception seven years ago had not President Woodward approved it so spontaneously, urged its completion with the greatest thoroughness, and given continued encouragement.

L. E. DICKSON.

November, 1918.

TABLE OF CONTENTS.

CHAPTER.	PAGE.
I. Perfect, multiply perfect, and amicable numbers.....	3
II. Formulas for the number and sum of divisors, problems of Fermat and Wallis.....	51
III. Fermat's and Wilson's theorems, generalizations and converses; symmetric functions of $1, 2, \dots, p-1$, modulo p	59
IV. Residue of $(u^{p-1}-1)/p$ modulo p	105
V. Euler's ϕ -function, generalizations; Farey series.....	113
VI. Periodic decimal fractions; periodic fractions; factors of $10^n \pm 1$	159
VII. Primitive roots, exponents, indices, binomial congruences.....	181
VIII. Higher congruences.....	223
IX. Divisibility of factorials and multinomial coefficients.....	263
X. Sum and number of divisors.....	279
XI. Miscellaneous theorems on divisibility, greatest common divisor, least common multiple.....	327
XII. Criteria for divisibility by a given number.....	337
XIII. Factor tables, lists of primes.....	347
✓XIV. Methods of factoring.....	357
XV. Fermat numbers $F_n = 2^{2^n} + 1$	375
XVI. Factors of $a^n \pm b^n$	381
XVII. Recurring series; Lucas' u_n, v_n	393
✓XVIII. Theory of prime numbers.....	413
XIX. Inversion of functions; Möbius' function $\mu(n)$; numerical integrals and derivatives.....	441
XX. Properties of the digits of numbers.....	453
Author index.....	467
Subject index.....	484

CHAPTER I.

PERFECT, MULTIPLY PERFECT, AND AMICABLE NUMBERS.

PERFECT, ABUNDANT, AND DEFICIENT NUMBERS.

By the aliquot parts or divisors of a number are meant the divisors, including unity, which are less than the number. A number, like $6 = 1 + 2 + 3$, which equals the sum of its aliquot divisors is called perfect (*vollkommen, vollständig*). If the sum of the aliquot divisors is less than the number, as is the case with 8, the number is called deficient (*diminute, defective, unvollkommen, unvollständig, mangelhaft*). If the sum of the aliquot divisors exceeds the number, as is the case with 12, the number is called abundant (*superfluus, plus quam-perfectus, redundantem, excédant, übervollständig, überflüssig, überschüssende*).

Euclid¹ proved that, if $p = 1 + 2 + 2^2 + \dots + 2^n$ is a prime, $2^n p$ is a perfect number. He showed that $2^n p$ is divisible by 1, 2, ..., 2^n , p , $2p$, ..., $2^{n-1}p$, but by no further number less than itself. By the usual theorem on geometrical progressions, he showed that the sum of these divisors is $2^n p$.

The early Hebrews^{1a} considered 6 to be a perfect number.

Philo Judeus^{1b} (first century A. D.) regarded 6 as the most productive of all numbers, being the first perfect number.

Nicomachus² (about A. D. 100) separated the even numbers (book I, chaps. 14, 15) into abundant (citing 12, 24), deficient (citing 8, 14), and perfect, and dwelled on the ethical import of the three types. The perfect (I, 16) are between excess and deficiency, as consonant sound between acuter and graver sounds. Perfect numbers will be found few and arranged with fitting order; 6, 28, 496, 8128 are the only perfect numbers in the respective intervals between 1, 10, 100, 1000, 10000, and they have the property of ending alternately in 6 and 8. He stated that Euclid's rule gives all the perfect numbers without exception.

Theon of Smyrna³ (about A. D. 130) distinguished between perfect (citing 6, 28), abundant (citing 12) and deficient (citing 8) numbers.

¹Elementa, liber IX, prop. 36. Opera, 2, Leipzig, 1884, 408.

^{1a}S. Rubin, "Sod Hasfiroth" (secrets of numbers), Wien, 1873, 59; citation of the Bible, Kings, II, 13, 19.

^{1b}Treatise on the account of the creation of the world as given by Moses, C. D. Young's transl. of Philo's works, London, 1854, vol. 1, p. 3.

²Nicomachi Gerasini arithmeticae libri duo. Nunc primum typis excusi, in lucem eduntur. Parisiis, 1538. In officina Christiani Wecheli. (Greek.)

Theologumena arithmeticae. Accedit Nicomachi Gerasini institutio arithmetica ad fidem codicum Monacensium emendata. Ed., Fridericus Astius. Lipsiae, 1817. (Greek.)

Nicomachi Geraseni Pythagorei introductionis arithmeticae libri ii. Recensvit Ricardus Hoche. Lipsiae, 1866. (Greek.)

³Theonis Smyrnaei philosophi Platonici expositio rerum mathematicarum ad legendum Platonem utilium. Ed., Ed. Hiller, Leipzig, 1878, p. 45.

Theonis Smyrnaei Platonici, Latin by Ismaele Bullialdo. Paris, 1644, chap. 32, pp. 70-72.

Iamblichus⁴ (about 283–330) repeated in effect the remarks by Nicomachus on perfect, abundant, and deficient numbers, but made erroneous additions. He stated that there is one and but one perfect number in the successive intervals between 1, 10, 100, . . . , 100000, etc., to infinity. “Examples of a perfect number are 6, and 28, and 496, and 8128, and the like numbers, alternately ending in 6 and 8.” He remarked that the Pythagoreans called the perfect number 6 marriage, and also health and beauty (on account of the integrity of its parts and the agreement existing in it).

Aurelius Augustinus⁵ (354–430) remarked that, 6 being the first perfect number, God effected the creation in 6 days rather than at once, since the perfection of the work is signified by the number 6. The sum of the aliquot parts of 9 falls short of it; likewise for 10. But the sum of the aliquot parts of 12 exceeds it.

Anicius Manlius Severinus Boethius⁶ (about 481–524), in a Latin exposition of the arithmetic of Nicomachus, stated that perfect numbers are rare, easily counted, and generated in a very regular order, while abundant (superfluos) and deficient (diminutos) numbers are found to an unlimited extent and not in regular order. The perfect numbers below 10000 are 6, 28, 496, 8128. And these numbers always end alternately in 6 and 8.

Munyo⁷ stated that Boethius added to Euclid’s idea of perfect number that of deficient (diminute) and abundant (redundantem) numbers.

Isidorus of Seville⁸ (570–636) distinguished even and odd numbers, perfect and abundant numbers, linear, flächen and Körper Zahlen (primes, products of two, products of three factors).

Alcuin⁹ (735–804), of York and Tours, explained the occurrence of the number 6 in the creation of the universe on the ground that 6 is a perfect number. The second origin of the human race arose from the deficient number 8; indeed, in Noah’s ark there were 8 souls from which sprung the entire human race, showing that the second origin was more imperfect than the first, which was made according to the number 6.

⁴Iamblichus Chalcidensis ex Coele-Syria in Nicomachi Geraseni arithmetica introductionem, et de Fato. Accedit Joachimi Camerarii explicatio in duos libros Nicomachi. Ed., Samuel Tennulius. Arnheimiae, 1668, pp. 43–47. (Greek text and Latin translation in parallel columns.)

Iamblichi in Nicomachi arithmetica introductionem liber ad fidem codicis Florentini. Ed., H. Pistelli. Lipsiae, 1894. (Greek.)

⁵De Civitate Dei, liber XI, cap. XXX, ed., B. Dombart, Lipsiae, 1877, I, p. 504. The reference by Frizzo²⁹ is to lib. II, cap. 39.

⁶Arithmetica boetij, Augsburg, 1488; Cologne, 1489; Leipzig, 1490; Venice, 1491–2, 1499; Paris, [1496, 1501], 1503, etc.; lib. 1, cap. 20, “De generatione numeri perfecti.”

Opera Boetii, Venice, 1491–2, etc.; ed., Friedlein, Leipzig, 1867.

⁷Institutiones arithmeticae ad percipiendam astrologiam et mathematicas facultates necessariae. Auctore Hieronymo Munyo, Valentiae, 1566, f. 5, verso.

⁸Incipit epistola Isidori iunioris hispalensis . . . Finit liber etymologiarum . . . [Augsburg, 1472]; Venice, 1483, etc. In this book of etymologies, arithmetic is treated very briefly in Book 3, beginning f. 15.

⁹Bibliotheca Rerum Germanicarum, tomus sextus: Monumenta Alcuiniana, Berlin, 1873, epistolae 259, pp. 818–821. Cf. Migne, Patrologiae, vol. 100, 1851, p. 665; Hankel, Geschichte Math., p. 311.

Thâbit ben Korrah,¹⁰ in a manuscript composed the last half of the ninth century, attributed to Pythagoras and his school the employment of perfect and amicable numbers in illustration of their philosophy. Let $s = 1 + 2 + \dots + 2^n$. Then (prop. 5), $2^n s$ is a perfect number if s is a prime; $2^n p$ is abundant if p is a prime $< s$, deficient if p is a prime $> s$, and the excess or deficiency of the sum of all the divisors over the number equals the difference of s and p . Let (prop. 6) p' and p'' be distinct primes > 2 ; the sum of the divisors $< N$ of $N = p'p''2^n$ is

$$a = (2^{n+1} - 1)(1 + p' + p'') + (2^n - 1)p'p''.$$

Hence N is abundant or deficient according as

$$a - N = (2^{n+1} - 1)(1 + p' + p'') - p'p'' > 0 \text{ or } < 0.$$

Hrotsvitha,¹¹ a nun in Saxony, in the second half of the tenth century, mentioned the perfect numbers 6, 28, 496, 8128.

Abraham Ibn Ezra^{11a} (†1167), in his commentary to the Pentateuch, Ex. 3, 15, stated that there is only one perfect number between any two successive powers of 10.

Rabbi Josef b. Jehuda Ankin^{11b}, at the end of the twelfth century, recommended the study of perfect numbers in the program of education laid out in his book "Healing of Souls."

Jordanus Nemorarius¹² (†1236) stated (in Book VII, props. 55, 56) that every multiple of a perfect or abundant number is abundant, and every divisor of a perfect number is deficient. He attempted to prove (VII, 57) the erroneous statement that all abundant numbers are even.

Leonardo Pisano, or Fibonacci, cited in his *Liber Abbaci*¹³ of 1202, revised about 1228, the perfect numbers

$$\frac{1}{2} 2^2(2^2 - 1) = 6, \quad \frac{1}{2} 2^3(2^3 - 1) = 28, \quad \frac{1}{2} 2^5(2^5 - 1) = 496,$$

excluding the exponent 4 since $2^4 - 1$ is not prime. He stated that by proceeding so, you can find an infinitude of perfect numbers.

¹⁰Manuscript 952, 2, Suppl. Arabe, Bibliothèque impériale, Paris. Textual transl., except of the proofs which are given in modern algebraic notation as foot-notes [as numbers were represented by line. in the manuscript], by Franz Woepcke, *Journal Asiatique*, (4), 20, 1852, 420-9.

¹¹See Ch. Magnin, *Théâtre de Hrotsvitha*, Paris, 1845.

^{11a}Mikrooth Gedoloth, Warsaw, 1874 ("Large Bible" in Hebrew). Samuel Ben Sáadias Ibn Motot, a Spaniard, wrote in 1370 a commentary on Ibn Ezra's commentary, *Perush ai Perush Ibn Ezra*, Venice, 1554, p. 19, noting the perfect numbers 6, 28, 496, 8128, and citing Euclid's rule. Steinschneider, in his book on Ibn Ezra, *Abh. Geschichte Math. Wiss.*, 1880, p. 92, stated that Ibn Ezra gave a rule for finding all perfect numbers. As this rule is not given in the *Mikrooth Gedoloth* of 1874, Mr. Ginsburg of Columbia University infers the existence of a fuller version of Ibn Ezra's commentary.

^{11b}Quoted by Gûdeman, *Das Jûdische Unterrichtswesen während der Spanisch Arabischen Periode*, Wien, 1873.

¹²In hoc opere contenta. *Arithmetica decem libris demonstrata Epitome i libris arithmeticos diui Seuerini Boetij . . .*, Paris, 1496, 1503, etc. It contains Jordanus' "Elementa arithmetica decem libris, demonstrationibus Jacobi Fabri Stapulensis," and "Jacobi Fabri Stapulensis epitome in duos libros arithmeticos diui Seuerini Boetij."

¹³Il *Liber Abbaci* di Leonardo Pisano. Roma, 1857, p. 283 (Seritti, vol. 1).

In the manuscript¹⁴ Codex lat. Monac. 14908, a part dated 1456 and a part 1461, the first four perfect numbers are given (f. 33') as usual and the fifth perfect number is stated correctly to be 33550336.

Nicolas Chuquet¹⁵ defined perfect, deficient, and abundant numbers, indicated a proof of Euclid's rule and stated incorrectly that perfect numbers end alternately in 6 and 8.

Luca Paciolo, de Borgo San Sepolcro,¹⁶ gave (f. 6) Euclid's rule, saying one must find by experiment whether or not the factor $1+2+4+\dots$ is prime, stated (f. 7) that the perfect numbers end alternately in 6 and 8, as 6, 28, 496, etc., to infinity. In the fifth article (ff. 7, 8), he illustrated the finding of the aliquot divisors of a perfect number by taking the case of the fourteenth perfect number 9007199187632128. He gave its half, then the half of the quotient, etc., until after 26 divisions by 2, the odd number 134217727, marked "Indivisibilis" [prime]. Dividing the initial number by these quotients, he obtained further factors [1, 2, ..., 2^{26} , but written at length]. The proposed number is said to be evidently perfect, since it is the sum of these factors [but he has not employed all the factors, since the above odd number equals $2^{27}-1$ and has the factor $2^3-1=7$]. Although Paciolo did not list the perfect numbers between 8128 and $90\dots8$, the fact that he called the latter the fourteenth perfect number implies the error expressly committed by Bovillus.²⁰

Thomas Bradwardin¹⁷ (1290-1349) stated that there is only one perfect number (6) between 1 and 10, one (28) up to 100, 496 up to 1000, 8128 up to 10000, from which these numbers, taken in order, end alternately in 6 and 8. He then gave Euclid's rule.

Faber Stapulensis¹⁸ or Jacques Lefèvre (born at Étapes 1455, †1537) stated that all perfect numbers end alternately in 6 and 8, and that Euclid's rule gives all perfect numbers.

Georgius Valla¹⁹ gave the first four perfect numbers and observed that

¹⁴The manuscript is briefly described by Gerhardt, Monatsber. Berlin Ak., 1870, 141-2. See *Catalogus codicum latinorum bibliothecae regiae Monacensis*, Tomi II, pars II, codices num. 11001-15028 complectus, Munich, 1876, p. 250. An extract of ff. 32'-34 on perfect numbers was published by Maximilian Curtze, *Bibliotheca Mathematica*, (2), 9, 1895, 39-42.

¹⁵*Triparty en la science des nombres*, manuscript No. 1436, Fonds Français, Bibliothèque Nationale de Paris, written at Lyons, 1484. Published by Aristide Marre, *Bull. Bibl. Storia Sc. Mat. et Fis.* 13 (1880), 593-659, 693-814; 14 (1881), 417-460. See Part 1, Ch. III, 3, 619-621, manuscript, ff. 20-21.

¹⁶*Summa de Arithmetica geometria proportioni et proportionalita*. [Summa . . . , Venice, 1494.] Toscolano, 1523 (two editions substantially the same).

¹⁷*Arithmetica thome brauardini. Tractatus perutilis*. In *arithmetica speculativa a magistro thoma brauardini ex libris euclidis boecij & aliorum qua optimne excerptus*. Parisiis, 1495, 7th unnumbered page.

Arithmetica Speculativa Thome Brauardini nuper mendis Plusculis tersa et diligenter Impressa, Parisiis [1502], 6th and 7th unnumbered pages. Also undated edition [1510], 3d page.

¹⁸*Epitome* (iii) of the arithmetic of Boethius in Faber's edition of Jordanus,¹² 1496, etc. Also in *Introductio Jacobi fabri Stapulensis in Arithmetecam diui Seuerini Boetij pariter Jordani*, Paris, 1503, 1507. Also in *Stapulensis, Jacobi Fabri, Arithmetica Boethi epitome*, Basileae, 1553, 40.

¹⁹*De expetendis et fvgiendis rebvs opvs*, Aldus, 1501. Liber I (= *Arithmeticae* I), Cap. 12.

"these happen to end in 6 or 8 . . . and these terminal numbers will always be found alternately."

Carolus Bovillus²⁰ or Charles de Bouvelles (1470–1553) stated that every perfect number is even, but his proof applies only to those of Euclid's type. He corrected the statement of Jordanus¹² that every abundant number is even, by citing 45045 [= 5·9·7·11·13] and its multiples. He stated that $2^n - 1$ is a prime if n is odd, explicitly citing 511 [= 7·73] as a prime. He listed as perfect numbers $2^{n-1}(2^n - 1)$, n ranging over all the odd numbers ≤ 39 [Cataldi⁴⁴ later indicated that 8 of these are not perfect]. He repeated the error that all perfect numbers end alternately in 6 and 8. He stated (f. 175, No. 25) that if the sum of the digits of a perfect number > 6 be divided by 9, the remainder is unity [proved for perfect numbers of Euclid's type by Cataldi,⁴⁴ p. 43]. He noted (f. 178) that any divisor of a perfect number is deficient, any multiple abundant. He stated (No. 29) that one or both of $6n \pm 1$ are primes and (No. 30) conversely any prime is of the form $6n \pm 1$ [Cataldi,⁴⁴ p. 45, corrects the first statement and proves the second]. He stated (f. 174) that every perfect number is triangular, being $2^n(2^n - 1)/2$.

Martinus²¹ gave the first four perfect numbers and remarked that they end alternately in 6 and 8.

Gasper Lax²² stated that the perfect numbers end alternately in 6 and 8.

V. Rodulphus Spoletanus²³ was cited by Cataldi,⁴⁴ with the implication of errors on perfect numbers. [Copy not seen.]

Girardus Ruffus²⁴ stated that every perfect number is even, that most odd numbers are deficient, that, contrary to Jordanus,¹² the odd number 45045 is abundant, and that for n odd $2^n - 1$ always leads to a perfect number, citing 7, 31, 127, 511, 2047, 8191 as primes [the fourth and fifth are composite].

Feliciano²⁵ stated that all perfect numbers end alternately in 6 and 8.

Regius²⁶ defined a perfect number to be an even number equal to the sum of its aliquot divisors, indicated that 511 and 2047 are composite, gave correctly 33550336 as the fifth perfect number, but said the perfect numbers

²⁰Caroli Bouilli Samarobrini Liber De Perfectis Numeris (dated 1509 at end), one (ff. 172–180) of 13 tracts in his work, *Que hoc volumine continetur: Liber de intellectu, . . . De Numeris Perfectis, . . .*, dated on last page, 1510, Paris, ex officina Henrici Stephani. Biography in G. Maupin, *Opinions et Curiosités touchant la Math.*, Paris, 1, 1901, 186–94.

²¹*Ars Arithmetica* Ioannis Martini, Silicei: in theoricen & praxim. 1513, 1514. *Arithmetica* Ioannis Martini, Scilicei, Paris, 1519.

²²*Arithmetica speculatiua magistri Gasparis Lax*. Paris, 1515, Liber VII, No. 87 (end).

²³*De proportionem proportionum dispytatio*, Rome, 1515.

²⁴*Divi Severini Boetii Arithmetica, dvobvs discreta libris*, Paris, 1521; ff. 40–44 of the commentary by G. Ruffus.

²⁵*Libro di Arithmetica & Geometria speculatiua & praticale: Composto per maestro Francesco Feliciano da Lazisio Veronese Intitulato Scala Grimaldelli: Nouamente stampato*. Venice, 1526 (p. 3), 1527, 1536 (p. 4), 1545, 1550, 1560, 1570, 1669, Padoua, 1629, Verona, 1563, 1602.

²⁶*Vtrivsqve Arithmetices, epitome ex uariis authoribus concinnata per Hvdalrichum Regium*. Strasburg, 1536. Lib. I, Cap. VI: De Perfecto. Hvdalrichvs Regius, Vtrivsqve. . . ex variis . . . , Friburgi, 1550 [and 1543], Cap. VI, fol. 17–18.

end alternately in 6 and 8. A multiple of an abundant or perfect number is abundant, a divisor of a perfect number is deficient.

Cardan²⁷ (1501–1576) stated that perfect numbers were to be formed by Euclid's rule and always end with 6 or 8; and that there is one between any two successive powers of ten.

De la Roche²⁸ stated in effect that $2^{n-1}(2^n - 1)$ is perfect for every odd n , citing in particular 130816 and 2096128, given by $n=9$, $n=11$. This erroneous law led him to believe that the successive perfect numbers end alternately in 6 and 8.

Noviomagus²⁹ or Neomagus or Jan Bronekhorst (1494–1570) gave Euclid's rule correctly and stated that among the first 10 numbers, 6 alone is perfect, . . . , among the first 10000 numbers, 6, 28, 496, 8128 alone are perfect, etc., etc. [implying falsely that there is one and but one perfect number with any prescribed number of digits]. In Lib. II, Cap. IV, is given the sieve (or crib) of Eratosthenes, with a separate column for the multiples of 3, a separate one for the multiples of 5, etc.

Willichius³⁰ (†1552) listed the first four perfect numbers and stated that to these are to be added a very few others, whose nature is that they end either in 6 or 8.

Michael Stifel³¹ (1487–1567) stated that all perfect numbers except 6 are multiples of 4, while $4(8-1)$, $16(32-1)$, $64(128-1)$, $256(512-1)$, etc., to infinity, are perfect [error, Kraft³⁵]. He later³² repeated the latter error, listing as perfect

$$2 \times 3, 4 \times 7, 16 \times 31, 64 \times 127, 256 \times 511, 1024 \times 2047,$$

“& so fort an ohn end.” Every perfect number is triangular.

Peletier³³ (1517–1582) stated (1549, V left; 1554, p. 20) that the perfect numbers end in 6 or 8, that there is a single perfect number between any two successive powers of 10, and (1549, C III left; 1554, pp. 270–1) that $4(8-1)$, $16(32-1)$, $64(128-1)$, $256(511)$, . . . are perfect. The first two statements were also given later by Peletier.³⁴

²⁷Hieronimi C. Cardani Medici Mediolanensis, *Practica Arithmetice, & Mensurandi singularis*. Milan, 1537, 1539; Nürnberg, 1541, 1542, Cap. 42, de proprietatibus numerorum mirificis. Opera IV, Lyon, 1663.

²⁸Larismetique & Geometrie de maistre Estienne de la Roche dict Ville Franche, *Nouuellement Imprimee & des fautes corrigees*, Lyon, 1538, fol. 2, verso. Ed. 1, 1520.

²⁹De Nymeris libri dvo . . . authore Ioanne Nouiomago, Paris, 1539, Lib. II, Cap. III. Reprinted, Cologne, 1544; Deventer, 1551. Edition by G. Frizzo, Verona, 1901, p. 132.

³⁰Iodoci Vvillichii Reselliani, *Arithmeticae libri tres*, Argentorati, 1540, p. 37.

³¹*Arithmetica Integra*, Norimbergae, 1544, ff. 10, 11.

³²Die Coss Christoffs Rudolffs Die schönen Exempeln der Coss Durch Michael Stifel Gebessert vnd sehr gemehrt, Königsperg in Preussen, 1553, Anhang Cap. I, f. 10 verso, f. 11 (f. 27 v.), and 1571.

³³L'Arithmetique de Iacques Peletier dv Mans, departie en quatre Liures, Poitiers, 1549, 1550, 1553. . . . , ff. 77 v, 78 r. Revue e augmentee par l' Auteur, Lion, 1554. . . . Troisieme edition, reueue et augmentee, par Jean de Tovrnes, 1607.

³⁴*Arithmeticae Practicae methodvs facilis*, per Gemmam Frisium, Medicum, ac Mathematicum conscripta . . . In eandem Ioannis Steinii & Iacobi Peletarii Annotationes. Antverpiae, 1581, p. 10.

Postello³⁵ stated erroneously that 130816 [=256·511] is perfect.

Lodoico Baëza³⁶ stated that Euclid's rule gives all perfect numbers.

Pierre Forcadel³⁷ (†1574) gave 130816 as the fifth perfect number, implying incorrectly that 511 is a prime.

Tartaglia³⁸ (1506–1559) gave an erroneous [Kraft⁸⁵] list of the first twenty perfect numbers, viz., the expanded forms of $2^{n-1}(2^n - 1)$, for $n=2$ and the successive odd numbers as far as $n=39$. He stated that the sums $1+2+4$, $1+2+4+8$, . . . are alternately prime and composite; and that the perfect numbers end alternately in 6 and 8. The third "notable property" mentioned is that any perfect number except 6 yields the remainder 1 when divided by 9.

Robert Recorde³⁹ (about 1510–1558) stated that all the perfect numbers under $6 \cdot 10^9$ are 6, 28, 496, 8128, 130816, 2096128, 33550336, 536854528 [the fifth, sixth, eighth of these are not perfect].

Petrus Ramus⁴⁰ (1515–1572) stated that in no interval between successive powers of 10 can you find more than one perfect number, while in many intervals you will find none. At the end of Book I (p. 29) of his *Arithmeticae libri tres*, Paris, 1555, Ramus had stated that 6, 28, 496, 8128 are the only perfect numbers less than 100000.

Franciscus Maurolycus⁴¹ (1494–1575) gave an argument to show that every perfect number is hexagonal and hence triangular.

Peter Bungus⁴² (†1601) gave (1584, *pars altera*, p. 68) a table of 20 numbers stated erroneously to be the perfect numbers with 24 or fewer digits [the same numbers had been given by Tartaglia³⁸]. In the editions of 1591, etc., p. 468, the table is extended to include a perfect number of 25 digits, one of 26, one of 27, and one of 28. He stated (1584, pp. 70–71; 1591, pp. 471–2) that all perfect numbers end alternately in 6 and 28; employing Euclid's formula, he observed that the product of a power of 2 ending in 4 by a number ending in 7 itself ends in 28, while the product of one ending in 6 by one ending in 1 ends in 6. He verified (1585, *pars*

³⁵Theoricæ Arithmetices Compendium à Guilielmo Postello, Lutetiae, 1552, a syllabus on one large sheet of arithmetic definitions.

³⁶Nvmerandi Doctrina, Lvtetiae, 1555, fol. 27–28.

³⁷L'Arithmetique de P. Forcadel de Beziers, Paris, 1556–7. Livre I (1556), fol. 12 verso.

³⁸La seconda Parte del General Trattato di Nvmeri, et Misvra di Nicolo Tartaglia, Vinegia, 1556, f. 146 verso.

L'Arithmetique de Nicolas Tartaglia Brescian . . . Recueillie, & traduite d'Italien en François, par Gvillavme Gosselin de Caen, . . . Paris, 1578, f. 98 verso, f. 99.

³⁹The Whetstone of witte, whiche is the seconde parte of Arithmetike, London, 1557, eighth unnumbered page.

⁴⁰Petri Rami Scholarum Mathematicarum, Libri unus et triginta, à Lazaro Schonero recogniti & emendati, Francofvrti, 1599, Libr. IV (Arith.), p. 127, and Basel, 1578.

⁴¹Arithmeticon libri duo, Venetiis, 1575, p. 10; 1580. Published with separate paging, at end of Opuscula mathematica.

⁴²Mysticae nvmerorum significationis liber in duas divisvs partes, R. D. Petro Bongo Canonico Bergomate avctore. Bergomi. Pars prior, 1583, 1585. Pars altera, 1584.

Petri Bungi Bergomatis Numerorum mysteria, Bergomi, 1591, 1599, 1614, Lutetiae Parisiorum, 1618, all four with the same text and paging. Classical and biblical citations on numbers (400 pages on 1, 2, . . . , 12). On the 1618 edition, see Fontés, Mém. Acad. Sc. Toulouse, (9), 5, 1893, 371–380.

prior, p. 238; 1591, p. 343) for the first seven numbers of his table [two being imperfect, however] that the sum of the digits of a perfect number exceeds by unity a multiple of 9. Every perfect number is triangular (1591, p. 270). Every multiple of a perfect number is abundant, every divisor deficient (1591, p. 464).

Unicornus⁴³ (1523–1610) cited Bungus and repeated his error that $2^{n-1}(2^n-1)$ is always perfect for n odd and that all perfect numbers end alternately in 6 and 8.

Cataldi⁴⁴ (1548–1626) noted in his Preface that Paciuolo's¹⁶ fourteenth perfect number 90...8 is in fact abundant since it arose from $1+2+4+\dots+2^{26}=134217727$, which is divisible by 7, whereas Paciuolo said it was prime. Citing the error of the latter, Bovillus,²⁰ and others, that all perfect numbers end alternately in 6 and 8, Cataldi observed (p. 42) that the fifth perfect number is 33550336 and the sixth is 8589869056, from $8191=2^{13}-1$ and $131071=2^{17}-1$, respectively, proved to be primes (pp. 12–17) by actually trying as possible divisor every prime less than their respective square roots. He gave (pp. 17–22) the corresponding work showing $2^{19}-1$ to be prime. He stated (p. 11) that 2^n-1 is a prime for $n=2, 3, 5, 7, 13, 17, 19, 23, 29, 31, 37$, remarking that the prime $n=11$ does not yield a perfect number since (p. 5) $2^{11}-1=2047=23\cdot 89$, while it is composite if n is composite. He proved (p. 8) that the perfect numbers given by Euclid's rule end in 6 or 8. He gave (pp. 28–40, 48) a table of all divisors of all even and odd numbers ≤ 800 , and a table of primes < 750 .

Georgius Henischiib⁴⁵ (1549–1618) stated that the perfect numbers end alternately in 6 and 8, and that one occurs between any two successive powers of 10. He applied Euclid's formula without restricting the factor 2^n-1 to primes.

Johan Rudolff von Graffenried⁴⁶ stated that all perfect numbers are given by Euclid's rule, which he applied without restricting 2^n-1 to primes, expressly citing 256×511 as the fifth perfect number. Every perfect number is triangular.

Bachet de Mézirac⁴⁷ (1581–1638) gave (f. 102) a lengthy proof of Euclid's theorem that 2^np is perfect if $p=1+2+\dots+2^n$ is a prime, but

⁴³De l'arithmetica vniversale del Sig. Ioseppo Vnicorno, Venetia, 1598, f. 57.

⁴⁴Trattato de nvmeri perfetti di Piero Antonio Cataldo, Bologna, 1603. According to the Preface, this work was composed in 1588. Cataldi founded at Bologna the *Academia Erigende*, the most ancient known academy of mathematics; his interest in perfect numbers from early youth is shown by the end of the first of his "due lettioni fatte nell' *Academia di Perugia*" (G. Libri, *Hist. Sc. Math. en Italie*, 2d ed., vol. 4, Halle, 1865, p. 91). G. Wertheim, *Bibliotheca Math.*, (3), 3, 1902, 76–83, gave a summary of the *Trattato*.

⁴⁵*Arithmetica Perfecta et Demonstrata*, Georgii Henischiib, Augsburg [1605], 1609, pp. 63–64.

⁴⁶*Arithmeticae Logistica Popularis Libri IIII*. In welchen der Algorithmus in gantzen Zahlen u. Fracturen . . . , Bern, 1618, 1619, pp. 236–7.

⁴⁷*Elementorum arithmeticonum libri XIII auctori D . . .*, a Latin manuscript in the Bibliothèque de l'Institut de France. On the inside of the front cover is a comment on the sale of the manuscript by the son of Bachet to Dalibert, treasurer of France. A general account of the contents of the manuscript was given by Henry, *Bull. Bibl. Storia Sc. Mat. e Fis.*, 12, 1879, pp. 619–641. The present detailed account of Book 4, on perfect numbers, was taken from the manuscript.

(f. 103, verso) is abundant if p is composite. Every multiple of a perfect or abundant number is abundant, every divisor of a perfect number is deficient (ff. 104 verso, 105). The product of two primes, other than 2×3 , is deficient (f. 105 verso). The odd number 945 is abundant, the sum of its aliquot divisors being 975 (f. 107). Commenting (f. 111 verso, f. 112) on the statement of Boethius⁶ and Cardan²⁷ that the perfect numbers end alternately in 6 and 8, he stated that the fourth is 8128 and the fifth is 2096128 [an error], the fifth not being $130816 = 256 \times 511$, since $511 = 7 \times 73$.

Jean Leurechon⁴⁸ (about 1591–1670) stated that there are only ten perfect numbers between 1 and 10^{12} , listed them (noting the admirable property that they end alternately in 6 and 8) and gave the twentieth perfect number. [They are the same as in Tartaglia's³⁸ list.]

Lantz⁴⁹ stated that the perfect numbers are $2(4-1)$, $4(8-1)$, $16(32-1)$, $64(128-1)$, $256(512-1)$, $1024(2048-1)$, etc.

Hugo Sempilius⁵⁰ or Semple (Scotland, 1594–Madrid, 1654) stated that there are only seven perfect numbers up to 40,000,000; they end alternately in 6 and 8.

Casper Ens⁵¹ stated that there are only seven perfect numbers $< 4 \cdot 10^7$, viz., 6, 28, 496, 8128, 130816, 1996128 [for 2096128], 33550336, and that they end alternately in 6 and 8.

Daniel Schwenter⁵² (1585–1636) made the same error as Casper Ens.⁵¹

Erycius Puteanus⁵³ quoted from Martiano Capella, lib. VII, De Nuptiis Philologiae, to the effect that the perfect number 6 is attributed to Venus; for it is made by the union of the two sexes, that is, from triad, which is male since it is odd, and from diad, which is feminine since it is even. Puteanus said that the perfect numbers in order are 6, 28, 496, 8128, 130816, 2096128, 33550336, and gave all their divisors [implying that 511, 2047, 8191 are primes], and stated that these seven and all the remaining end alternately in 6 and 8. Between any two successive powers of 10 is one perfect number. That they are all triangular adds perfection to the perfect.

Joannes Broscius⁵⁴ or Brocki remarked that there is no perfect number between 10000 and 10000000, contrary to Stifel,³¹ Bungus,⁴² Sempilius,⁵⁰ Puteanus,⁵³ and the author of *Selectarum Propositionum Mathematicarum*, quas propugnavit, Mussiponti, Anno 1622, Maximilianus Willibaldus, Baro

⁴⁸Récréations mathématiques, Pont-à-Mousson, 1624; London, 1633, 1653, 1674 (these three English editions by Wm. Oughtred), p. 92. The authorship is often attributed to Leurechon's pupil Henry Van Etten, whose name is signed to the dedicatory epistle. Cf. Poggenдорff, Handwörterbuch, 1863, 2, p. 250 (under C. Mydorge); Bibliothèque des écrivains de la compagnie de Jésus, par A. de Backer, 2, 1872, 731; Biographie Générale, 31, 1872, 10.

⁴⁹Institutionum Arithmeticarum libri quatuor à Ioanne Lantz, Coloniae Agrippinae, 1630, p. 54.

⁵⁰De Mathematicis Disciplinis libri Duodecim, Antverpiae, 1635, Lib. 2, Cap. 3, N. 10, p. 46. There is (pp. 263–5) an index of writers on geometry and one for arithmetic.

⁵¹Thaumaturgus Math., Munich, 1636, p. 101; Coloniae, 1636, 1651; Venice, 1706.

⁵²Deliciae Physico-Mathematicae oder Mathemat: vnd Philosophische Erquickstunden, part I (574 pp.), Nürnberg, 1636, p. 108.

⁵³De Bissexto Liber: nova temporis facula qua intercalandi arcana . . . Lovanii, 1637; 1640, pp. 103–7. Reproduced by J. G. Graevius, Thesaurus Antiquitatum Romanarum (12 vols., 1694–9), Lugduni Batavorum, vol. 8.

in Waldpurg. While they considered 511×256 and 2047×1024 as perfect, 511 has the factor 7, and (as pointed out to him by Stanislaus Pudlowski) 2047 has the factor 23. Broscius stated that

$2^n - 1$ has the factor 3 5 7 11 13 17 19 23 29 31
if n is a multiple of 2 4 3 10 12 8 18 11 28 5.

The contents of the second dissertation are given below under the date 1652.

René Descartes,⁵⁵ in a letter to Mersenne, November 15, 1638, thought he could prove that every even perfect number is of Euclid's type, and that every odd perfect number must have the form ps^2 , where p is a prime. He saw no reason why an odd perfect number may not exist. For $p = 22021$, $s = 3 \cdot 7 \cdot 11 \cdot 13$, ps^2 would be perfect if p were prime [but $p = 61 \cdot 19^2$]. In a letter to Frenicle, January 9, 1639, Oeuvres, 2, p. 476, he expressed his belief that an odd perfect number could be found by replacing 7, 11, 13 in s by other values.

Fermat⁵⁶ stated that he possessed a method of solving all questions relating to aliquot parts. Citing this remark, Frenicle⁵⁷ challenged Fermat to find a perfect number of 20 or 21 digits. Fermat⁵⁸ replied that there is none with 20 or 21 digits, contrary to the opinion of those who believe that there is a perfect number between any two consecutive powers of 10.

Fermat,⁵⁹ in a letter to Mersenne, June (?), 1640, stated three propositions which he had proved not without considerable trouble and which he called the basis of the discovery of perfect numbers: if n is composite, $2^n - 1$ is composite; if n is a prime, $2^n - 2$ is divisible by $2n$, and $2^n - 1$ is divisible by no prime other than those of the form $2kn + 1$ [cf. Euler⁸⁷]. For example, $2^{11} - 1 = 23 \cdot 89$, $2^{37} - 1$ has the factor 223. Also $2^{23} - 1$ has the factor 47, Oeuvres, 2, p. 210, letter to Frenicle, October 18, 1640.

Mersenne⁶⁰ (1588–1648) stated that, of the 28 numbers* exhibited by

⁵⁴De numeris perfectis disceptatio qua ostenditur a decem millibus ad centies centena millia, nullum esse perfectum numerum atque ideo ab unitate usque ad centies centena millia quatuor tantum perfectos numerari, Amsterdam, 1638. Reproduced as the first (pp. 115–120) of two dissertations on perfect numbers, they forming pp. 111–174 of *Apologia pro Aristotele & Evclide, contra Petrum Ramum, & alios. Addititiae sunt Dvae Disceptationes de Numeris Perfectis. Authore Ioanne Broscio, Dantisci, 1652* (with a somewhat different title, Amsterdam, 1699).

⁵⁵Oeuvres de Descartes, II, Paris, 1898, p. 429.

⁵⁶Oeuvres de Fermat, 2, Paris, 1894, p. 176; letter to Mersenne, Dec. 26, 1638.

⁵⁷Oeuvres de Fermat, 2, p. 185; letter to Mersenne, March, 1640.

⁵⁸Oeuvres, 2, p. 194; letter to Mersenne, May (?), 1640.

⁵⁹Oeuvres de Fermat, 2, pp. 198–9; *Varia Opera Math. d. Petri de Fermat, Tolosae, 1679*, p. 177; *Précis des Oeuvres math. de P. Fermat et de l'Arithmétique de Diophante*, par E. Brassinne, Mém. Ac. Imp. Sc. Toulouse, (4), 3, 1853, 149–150.

⁶⁰F. Marini Mersenni minimi Cogitata Physico Mathematica, Parisiis, 1644. Praefatio Generalis, No. 19. C. Henry (Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 524–6) believed that these remarks were taken from letters from Fermat and Frenicle, and that Mersenne had no proof. A similar opinion was expressed by W. W. Rouse Ball, *Messenger Math.*, 21, 1892, 39 (121). On documents relating to Mersenne see *l'intermédiaire des math.*, 2, 1895, 6; 8, 1901, 105; 9, 1902, 101, 297; 10, 1903, 184. Cf. Lucas.¹¹⁸

*Only 24 were given by Bungus. While his table has 28 lines, one for each number of digits, there are no entry of numbers of 5, 11, 17, 23 digits.

Bungus,⁴² chap. 28, as perfect numbers, 20 are imperfect and only 8 are perfect:

$$6, \quad 28, \quad 496, \quad 8128, \quad 23550336 \text{ [for } 33 \dots], \quad 8589869056, \\ 137438691328, \quad 2305843008139952128,$$

which occur at the lines marked 1, 2, 3, 4, 8, 10, 12 and 29 [for 19] of Bungus' table [indicating the number of digits]. Perfect numbers are so rare that only eleven are known, that is, three different from those of Bungus; nor† is there any perfect number other than those eight, unless you should surpass the exponent 62 in $1+2+2^2+\dots$. The ninth perfect number is the power with the exponent 68 less 1; the tenth, the power 128 less 1; the eleventh, the power 258 less 1, *i. e.*, the power 257, decreased by unity, multiplied by the power 256. [The first 11 perfect numbers are thus said to be $2^{n-1}(2^n-1)$ for $n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, in error as to $n=61, 67, 89, 107$ at least.] He who would find 11 others will know that all analysis up to the present will have been exceeded, and will remember in the meantime that there is no perfect number from the power 17000 to 32000, and no interval of powers can be assigned so great but that it can be given without perfect numbers. For example, if the exponent be 1050000, there is no larger exponent n up to 2090000 for which 2^n-1 is a prime. One of the greatest difficulties in mathematics is to exhibit a prescribed number of perfect numbers; and to tell if a given number of 15 or 20 digits is prime or not, all time would not suffice for the test, whatever use is made of what is already known.

Mersenne⁶¹ stated that 2^p-1 is a prime if p is a prime which exceeds by 3, or by a smaller number, a power of 2 with an even exponent. Thus 2^7-1 is a prime since $7=2^2+3$; again, since $67=3+2^6$, $2^{67}+1=1\dots7$ [for $2^{67}-1$] is a prime and leads to a perfect number [error corrected by Cole¹⁷³]. Understand this only of primes 2^p-1 . Wherefore this property does not belong to the prime 5, but to 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, and all such. Numbers expressible as the sum or difference of two squares in several ways are composite, as $65=1+64=16+49$. As he speaks of Frenicle's knowledge of numbers, at least part of his results are doubtless due to the latter.

In 1652, J. Broschius (Apologia,⁵⁴ p. 121) observed that while perfect numbers were deduced by Euclid from geometrical progressions, they may be derived from arithmetical progressions:

$$6=1+2+3, \quad 28=1+2+3+4+5+6+7, \quad 496=1+2+3+\dots+31.$$

†Neque enim vllus est alius perfectus ab illis octo, nisi superes exponentem numerum 62, progressionis duplae ab 1 incipientis. Nonus enim perfectus est potestas exponentis 68, minus 1. Decimus, potestas exponentis 128, minus 1. Vndecimus denique, potestas 258, minus 1, hoc est potestas 257, unitate decurtata, multiplicata per potestatem 256.

⁶¹F. Marini Mersenni Novarvm Observationvm Physico-Mathematicarum, Tomvs III, Parisiis, 1647, Cap. 21, p. 182. The Reflectiones Physico-Math. begin with p. 63; Cap. 21 is quoted in Oeuvres de Fermat, 4, 1912, pp. 67-8.

He stated that while perfect numbers end with 6 or 28, the proof by Bungus⁴² does not show that they end alternately with 6 and 28, since Bungus included imperfect as well as perfect numbers. The numbers 130816 and 2096128, cited as perfect by Puteanus,⁵³ are abundant. After giving a table of the expanded form of 2^n for $n=0, 1, \dots, 100$, Broscius (p. 130, seq.) gave a table of the prime divisors of 2^n-1 ($n=1, \dots, 100$), but showing no prime factor when n is any one of the primes, other than 11 and 23, less than 100. For $n=11$, the factors are 23, 89; for $n=23$, the factor 47 is given. Thus omitting unity, there remain only 23 numbers out of the first hundred which can possibly generate perfect numbers. Contrary to Cardan,²⁷ but in accord with Bungus,⁴² there is (p. 135) no perfect number between 10^4 and 10^5 . Of Bungus' 24 numbers, only 10 are perfect (pp. 135-140): those with 1, 2, 3, 4, 8, 10, 12, 18, 19, 22 digits, and given by $2^{n-1}(2^n-1)$ for $n=2, 3, 5, 7, 13, 17, 19, 29, 31, 37$, respectively. The primality of the last three was taken on the authority of unnamed predecessors.

There are only 21 abundant numbers between 10 and 100, and all of them are even; the only odd abundant number <1000 is 945, the sum of whose aliquot divisors is 975 (p. 146). The statement by Lucas, *Théorie des nombres*, 1, Paris, 1891, p. 380, Ex. 5, that $3^3 \cdot 5 \cdot 79$ [deficient] is the smallest abundant number is probably a misprint for $945=3^3 \cdot 5 \cdot 7$. This error is repeated in *Encyclopédie Sc. Math.*, I, 3, Fas. 1, p. 56.

Johann Jacob Heinlin⁶² (1588-1660) stated that the only perfect numbers $<4 \cdot 10^7$ are 6, 28, 496, 8128, 130816, 2096128, 33550336, and that all perfect numbers end alternately in 6 and 8.

Andrea Tacquet⁶³ (Antwerp, 1612-1660) stated (p. 86) that Euclid's rule gives all perfect numbers. Referring to the 11 numbers given as perfect by Mersenne,⁶⁰ Tacquet said that the reason why not more have been found so far is the greatness of the numbers 2^n-1 and the vast labor of testing their primality.

Frenicle⁶⁴ stated in 1657 that Euclid's formula gives all the even perfect numbers, and that the odd perfect numbers, if such exist, are of the form pk^2 , where p is a prime of the form $4n+1$ [cf. Euler⁹⁸].

Frans van Schooten⁶⁵ (the younger, 1615-1660) proposed to Fermat that he prove or disprove the existence of perfect numbers not of Euclid's type.

Joh. A. Leuneschlos⁶⁶ remarked that the infinite multitude of numbers contains only ten perfect numbers; he who will find ten others will know

⁶²Joh. Jacobi Heinlini, *Synopsis Math. praeicipuas totius math.* . . . Tubingae, 1653. *Synopsis Math. Universalis*, ed. III, Tubingae, 1679, p. 6. English translation of last by Venterus Mandey, London, 1709, p. 5.

⁶³*Arithmeticae Theoria et Praxis*, Lovanii, 1656 and 1682 (same paging), [1664, 1704]. His *opera math.*, Antwerpiae, 1669, does not contain the *Arithmetic*.

⁶⁴Correspondence of Chr. Huygens, No. 389; *Oeuvres de Fermat*, 3, Paris, 1896, p. 567.

⁶⁵*Oeuvres de Huygens*, II, Correspondence, No. 378, letter from Schooten to J. Wallis, Mar. 18, 1658. *Oeuvres de Fermat*, 3, Paris, 1896, p. 558.

⁶⁶*Mille de Quantitate Paradoxa Sive Admiranda*, Heildelbergae, 1658, p. 11, XLVI, XLVII.

that he has surpassed all analysis up to the present. Goldbach⁶⁷ called Euler's attention to these remarks and stated that they were probably taken from Mersenne, the true sense not being followed.

Wm. Leybourn⁶⁸ listed as the first ten perfect numbers and the twentieth those which occur in the table of Bungus.⁴² "The number 6 hath an eminent Property, for his parts are equal to himself."

Samuel Tennulius, in his notes (pp. 130-1) on Iamblicus,⁴ 1668, stated that the perfect numbers end alternately in 6 and 8, and included $130816 = 256 \cdot 511$ and $2096128 = 1024 \cdot 2047$ among the perfect numbers.

Tassius⁶⁹ stated that all perfect numbers end in 6 or 8. Any multiple of a perfect or abundant number is abundant, any divisor of a perfect number is deficient. He gave as the first eight known perfect numbers the first eight listed by Mersenne.⁶⁰

Joh. Wilh. Pauli⁷⁰ (Philatrus) noted that if $2^n - 1$ is a prime, n is, but not conversely. For $n = 2, 3, 5, 7, 13, 17, 19$, $2^n - 1$ is a prime; but $2^{11} - 1$ is divisible by 23, $2^{23} - 1$ by 47, and $2^{41} - 1$ by 83, the three divisors being $2n + 1$.

G. W. Leibniz⁷¹ quoted in 1679 the facts stated by Pauli and set himself the problem to find the basis of these facts. Returning about five years later to the subject of perfect numbers, Leibniz implied incorrectly that $2^p - 1$ is a prime if and only if p is.

Jean Prestet⁷² (†1690) stated that the fifth, . . . , ninth perfect numbers are 23550336 [for 33 . . .], 8589869056, 137438691328, 238584300813952128 [for 2305 . . . 39952128], $2^{513} - 2^{256}$.

[Hence $2^{n-1}(2^n - 1)$ for $n = 13, 17, 19, 31, 257$. The numerical errors were noted by E. Lucas,¹²⁴ p. 784.]

Jacques Ozanam⁷³ (1640-1717) stated that there is an infinitude of perfect numbers and that all are given by Euclid's rule, which is to be applied only when the odd factor is a prime.

Charles de Neugeglise⁷⁴ proved that the products $3 \cdot 4, \dots, 8 \cdot 9$ of two consecutive numbers are abundant. All multiples of 6 or an abundant number are abundant.

⁶⁷Correspondence Math. Phys., ed., Fuss, I, 1843; letters to Euler, Oct. 7, 1752 (p. 584), Nov. 18 (p. 593).

⁶⁸Arithmetical Recreations; or Enchriridion of Arithmetical Questions both Delightful and Profitable, London, 1667, p. 143.

⁶⁹Arithmeticae Empiricae Compendium, Johannis Adolphi Tassii. Ex recensione Henrici Siveri, Hamburgi, 1673, pp. 13, 14.

⁷⁰De numero perfecto, Leipzig, 1678, Magister-disputation.

⁷¹Manuscript in the Hannover Library. Cf. D. Mahnke, Bibliotheca Math., (3), 13, 1912-3, 53-4, 260.

⁷²Nouveaux elemens des Mathematiques, ou Principes generaux de toutes les sciences, Paris, 1689, I, 154-5.

⁷³Recreations mathematiques et physiques, Paris and Amsterdam, 2 vols., 1696, I, 14, 15.

⁷⁴Traité methodique et abrégé de toutes les mathématiques, Trevoux, 1700, tome 2 (L'arithmétique ou Science des nombres), 241-8.

John Harris,⁷⁵ D. D., F. R. S., stated that there are but ten perfect numbers between unity and one million of millions.

John Hill⁷⁶ stated that there are only nine perfect numbers up to a hundred thousand million. He gave (pp. 147-9) a table of values of 2^n for $n=1, \dots, 144$.

Christian Wolf⁷⁷ (1679-1754) discussed perfect numbers of the form $y^n x$ [where x, y are primes]. The sum of its aliquot parts is

$$1 + y + \dots + y^n + x + yx + \dots + y^{n-1}x,$$

which must equal $y^n x$. Thus

$$x = (1 + y + \dots + y^n)/d, \quad d = y^n - 1 - y - \dots - y^{n-1}.$$

He stated* that x is an integer only when $d=1$, and that this requires $y=2$, $x=1+2+\dots+2^n$. Then if this x is a prime, $2^n x$ is a perfect number. This is said to be the case for $n=8$ and $n=10$, since $2^9-1=511$ and $2^{11}-1=2047$ are primes, errors pointed out by Euler.⁸³ A. G. Kästner⁷⁸ was not satisfied with the argument leading to the conclusion $y=2$.

Jacques Ozanam⁷⁹ listed as perfect numbers

$$2(4-1), 4(8-1), 16(32-1), 64(128-1), 256(512-1), 1024(2048-1), \dots$$

without explicit mention of the condition that the final factor shall be prime, and stated that perfect numbers are rare, only ten being known, and all end in 6 and 8 alternately. [Criticisms by Montucla,⁹⁹ Gräson.¹⁰⁰]

Johann Georg Liebnecht⁸⁰ said there were scarcely 5 or 6 perfect numbers up to 4.10^7 ; they always end alternately in 6 and 8.

Alexander Malcolm⁸¹ observed that it is not yet proved that there is no perfect number not in Euclid's set. He stated that, if pA is a perfect number, where p is a prime, and if $M < p$ and M is not a factor of A , then MM is an abundant number [probably a misprint for MA , as the conditions are satisfied when $p=7$, $A=4$, $M=5$, and $MA=20$ is abundant, while $M^2=25$ is deficient].

Christian Wolf⁸² made the same error as Casper Ens.⁵¹

⁷⁵Lexicon Technicum, or an Universal English Dictionary of Arts and Sciences, vol. I, London, 1704; ed. 5, vol. 2, London, 1736.

⁷⁶Arithmetik, London, ed. 2, 1716, p. 3.

⁷⁷Elementa Matheseos Universae, Halae Magdeburgicae, vol. I, 1730 and 1742, pp. 383-4, of the five volume editions [first printed 1713-41]; vol. I, 1717, 315-6, of the two volume edition. Quoted, with other errors, Ladies' Diary, 1733, Q. 166; Leybourn's ed., 1, 1817, 218; Hutton's ed., 2, 1775, 10; Diarian Repository, by Soc. Math., 1774, 289.

*"Jam ut x sit numerus integer, nec in casu speciali, si y per numerum explicetur, numerus partium aliquotarum diversus sit a numero earundem in formula generali; necesse est ut $d=1$."

⁷⁸Math. Anfangsgründe, I, 2 (Fortsetzung der Rechenkunst, ed. 2, 1801, 546-8).

⁷⁹Recreations math., new ed. of 4 vols., 1723, 1724, 1735, etc., I, 29-30.

⁸⁰Grund-Sätze der gesammten Math. Wiss. u. Lehren, Giessen u. Franckfurt, 1724, p. 21.

⁸¹A new system of arithmetik, theoretical & practical, London, 1730, p. 394.

⁸²Mathematisches Lexicon, I, 1734 (under Vollkommen Zahl).

Leonard Euler⁸³ (1707–1783) noted that $2^n - 1$ may be composite for n a prime; for instance, $2^{11} - 1 = 23 \cdot 89$, contrary to Wolf.⁷⁷ If $n = 4m - 1$ and $8m - 1$ are primes, $2^n - 1$ has the factor $8m - 1$, so that $2^n - 1$ is composite for $n = 11, 23, 83, 131, 179, 191, 239$, etc. [Proof by Lucas.¹²³] Furthermore, $2^{37} - 1$ has the factor 223, $2^{43} - 1$ the factor 431, $2^{29} - 1$ the factor 1103, $2^{73} - 1$ the factor 439, etc. “However, I venture to assert that aside from the cases noted, every prime less than 50, and indeed than 100, makes $2^{n-1}(2^n - 1)$ a perfect number, whence the eleven values 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47 of n yield perfect numbers. I derived these results from the elegant theorem, of whose truth I am certain, although I have no proof: $a^n - b^n$ is divisible by the prime $n + 1$, if neither a nor b is.” [For later proofs by Euler, see Chapter III on Fermat’s theorem.] Euler’s errors as to $n = 41$ and 47 were corrected by Winsheim,⁹⁰ Euler⁹³ himself, and Plana.¹¹⁰

Michael Gottlieb Hansch⁸⁴ stated that $2^n - 1$ is a prime if n is any of the twenty-two primes ≤ 79 [error, Winsheim,⁹⁰ Kraft⁹³].

George Wolfgang Kraft⁸⁵ corrected Stifel’s³¹ error that 511·256 is perfect and the error of Ozanam (*Elementis algebrae*, p. 290) that the sum of all the divisors of 2^{4n} is a prime, by noting that the sum for $n = 2$ is $511 = 7 \cdot 73$; and noted that false perfect numbers were listed by Ozanam.⁷⁹ Kraft presented (pp. 9–11) an incomplete proof, communicated to him by Tobias Maier [cf. Fontana¹⁰¹], that every perfect number is of Euclid’s type. Let $1, m, n, \dots, p, A, \dots$ be the aliquot parts of any perfect number pA , where p and A are the middle factors [as 4 and 7 in 28]. Then

$$1 + m + n + r + q + p + A + \frac{pA}{q} + \frac{pA}{r} + \frac{pA}{n} + \frac{pA}{m} = pA.$$

Solving for A , he stated that the denominator must be unity, whence $p = 2q/D$, $D = q - 1 - q/r - q/n - q/m$. Again, $D = 1$, whence $q = 2r/D'$, $D' = r - 1 - r/n - r/m$. From $D' = 1$, $r = 2n/D''$, $D'' = n - 1 - n/m$. From $D'' = 1$, $n = 2m/(m - 1)$, $m - 1 = 1$, $m = 2$, $n = 4$, $r = 8$, etc. Thus the aliquot parts up to the middle must be the successive powers of 2, and A must be a prime, since otherwise there would be new divisors. For $p = 2^{n-1}$, we get $A = 2^n - 1$. Kraft observed that if we drop from Tartaglia’s³⁸ list of 20 numbers those shown to be imperfect by Euler’s⁸³ results, we have left only eight perfect numbers $2^{n-1}(2^n - 1)$ for $n \leq 39$, viz., those for $n = 2, 3, 5, 7, 13, 17, 19, 31$. For these, other than the first, as well as for the false ones of Tartaglia, if we add the digits, then add the digits of that sum, etc., we finally get unity (p. 14) [proof by Wantzel¹⁰⁶]. All perfect numbers end in 6 or 28.

⁸³Comm. Acad. Petropol., 6, 1738, ad annos 1732–3, p. 103. *Commentationes Arithmeticae Collectae*, I, Petropoli, 1849, p. 2.

⁸⁴Epistola ad mathematicos de theoria arithmetices nouis a se inuentis aucta, Vindobonae [Vienna], 1739.

⁸⁵De numeris perfectis, Comm. Acad. Petrop., 7, 1740, ad annos 1734–5, 7–14.

Johann Christoph Heilbronner⁸⁶ stated that the perfect numbers up to $4 \cdot 10^7$ are 6, 28, 496, 8128, 130816, 2096128. "The fathers of the early church and many writers always held this number 6 in high esteem. God completed the creation in 6 days and since all things created by Him came out perfect, he wished the work of creation completed according to the number 6 as being a perfect number."

L. Euler⁸⁷ deduced from Fermat's theorem, which he here proved by use of the binomial theorem, the result* that, if m is a prime, $2^m - 1$, when composite, has no prime factors other than those of the form $mn + 1$.

J. Landen⁸⁸ noted that 196 is the least number $4x^n$, where x is prime, the sum of whose aliquot parts exceeds the number by 7.

L. Euler⁸⁹ gave a table of the prime factors of $2^n - 1$ for $n \leq 37$.

C. N. de Winsheim⁹⁰ noted that $2^{47} - 1$ has the factor 2351, and stated that $2^n - 1$ is a prime for $n = 2, 3, 5, 7, 13, 17, 19, 31$, composite for the remaining $n < 48$, but was doubtful as to $n = 41$, thus reducing the list of perfect numbers given by Euler⁸³ by one or perhaps two. He suspected that $n = 41$ leads to an imperfect number since it was excluded by the acute Mersenne,⁶⁰ who gave instead $2^{66}(2^{67} - 1)$ as the ninth perfect number. He remarked that the basis of Mersenne's assertion is doubtless to be found in the stupendous genius of Mersenne which perhaps recognized more truths than he could demonstrate. He discussed the error of Hansch⁸⁴ that $2^n - 1$ is a prime if n is a prime ≤ 79 .

G. W. Kraft⁹¹ considered perfect numbers AP , where P is a prime [not dividing A]. Thus $a(P+1) = 2AP$, where a is the sum of all the divisors of A . Hence $a/(2A - a)$ equals the prime P . Let $2A - a = 1$, a property holding for $A = 2^m$. Then $P = 2^{m+1} - 1$ and the resulting numbers are of Euclid's type.

L. Euler,⁹² in a letter to Goldbach, October 28, 1752, stated that he knew only seven perfect numbers, viz., $2^{p-1}(2^p - 1)$ for $p = 2, 3, 5, 7, 13, 17, 19$, and was uncertain whether $2^{31} - 1$ is prime or not (a factor is necessarily of the form $64n + 1$ and none are < 2000).

⁸⁶*Historia matheseos universae. Accedit recensio elementorum compendiorum et operum math. atque historia arithmetices ad nostra tempora*, Lipsiae, 1742, 755-6. There is a 63-page list of arithmetics of the 16th century.

⁸⁷*Novi Comm. Ac. Petrop.*, 1, 1747-8, 20; *Comm. Arith.*, I, 56, § 39.

*We may simplify the proof by using the fact that 2 belongs to an exponent e modulo p (p a prime) such that e divides $p - 1$. For, if p is a factor of $2^m - 1$, m is a multiple of e , whence e equals the prime m . Thus $p - 1 = nm$. If we take $m > 2$, we see that n is even since p is odd and conclude with Fermat⁵⁹ that, if m is an odd prime, $2^m - 1$ is divisible by no primes other than those of the form $2km + 1$.

⁸⁸*Ladies' Diary*, 1748, Question 305. The *Diarian Repository*, Collection of all the mathematical questions from the *Ladies' Diary*, 1704-1760, by a society of mathematicians, London, 1774, 509. *Hutton's The Diarian Miscellany* (from *Ladies' Diary*, 1704-1773), London, 1775, vol. 2, 271. *Leybourn's Math. Quest.* proposed in *Ladies' D.*, 2, 1817, 9-10.

⁸⁹*Opuscula varii argumenti*, Berlin, 2, 1750, 25; *Comm. Arith.*, 1, 1849, 104.

⁹⁰*Novi Comm. Ac. Petrop.*, 2, 1751, ad annum 1749, mem., 68-99.

⁹¹*Ibid.*, mem., 112-3.

⁹²*Corresp. Math. Phys.* (ed., Fuss), I, 1843, 590, 597-8.

G. W. Kraft⁹³ stated (p. 114) that Euler had communicated to him privately in 1741 the fact that $2^{47} - 1$ is divisible by 2351. He stated (p. 121) that if $2^p - 1$ is composite (p being prime), it has a factor of the form $2q^m p + 1$, where q is a prime [including unity], using as illustrations the factorizations noted by Euler.⁹³ Of the numbers $2^n - 1$, n a prime ≤ 71 , stated to be prime by Hansch,⁸⁴ six are composite, while the cases 53, . . . , 71 are in doubt (p. 115).

A. Saverien⁹⁴ repeated the remarks by Ens⁵¹ without reference.

L. Euler⁹⁵ stated in a letter to Bernoulli that he had verified that $2^{31} - 1$ is a prime by examining the primes up to 46339 which are contained in the possible forms $248n + 1$ and $248n + 63$ of divisors.

L. Euler⁹⁶ gave a prime factor of $2^n \pm 1$ for various values of n , but no new cases $2^n - 1$ with n a prime.

L. Euler,⁹⁷ in a posthumous paper, proved that every even perfect number is of Euclid's type. Let $a = 2^n b$ be perfect, where b is odd. Let B denote the sum of the divisors of b . The sum $(2^{n+1} - 1)B$ of the divisors of a must equal $2a$. Thus $b/B = (2^{n+1} - 1)/2^{n+1}$, a fraction in its lowest terms. Hence $b = (2^{n+1} - 1)c$. If $c = 1$, $b = 2^{n+1} - 1$ must be a prime since the sum of its divisors is $B = 2^{n+1}$, whence Euclid's formula. If $c > 1$, the sum B of the divisors of b is not less than $b + 2^{n+1} - 1 + c + 1$; hence

$$\frac{B}{b} \geq \frac{2^{n+1}(c+1)}{b} > \frac{2^{n+1}}{2^{n+1}-1},$$

contrary to the earlier equation. The proof given in another posthumous paper by Euler⁹⁸ is not complete.

L. Euler⁹⁸ proved that any odd perfect number must be of the form $r^{4\lambda+1}P^2$, where r is a prime of the form $4n+1$ [Frenicle⁶⁴]. Express it as a product $ABC \dots$ of powers of distinct primes. Denote by a, b, c, \dots the sums of the divisors of A, B, C, \dots , respectively. Then $abc \dots = 2ABC \dots$. Thus one of the numbers a, b, \dots , say a , is the double of an odd number, and the remaining ones are odd. Thus B, C, \dots are even powers of primes, while $A = r^{4\lambda+1}$. In particular, no odd perfect number has the form $4n+3$. Amplifications of this proof have been given by Lionnet,¹²⁸ Stern,¹³⁷ Sylvester,¹⁴⁹ Lucas.¹⁵⁷ See also Liouville³⁰ in Chapter X.

Montucla⁹⁹ remarked that Euclid's rule does not give as many perfect numbers as believed by various writers; the one often cited [Paciuolo¹⁶] as the fourteenth perfect number is imperfect; the rule by Ozanam⁷⁹ is false since 511 and 2047 are not primes.

⁹³Novi Comm. Ac. Petrop., 3, 1753, ad annos 1750-1.

⁹⁴Dictionnaire universel de math. et physique, two vols., Paris, 1753, vol. 2, p. 216.

⁹⁵Nouv. Mém. Acad. Berlin, année 1772, hist., 1774, p. 35; Euler, Comm. Arith., 1, 1849, 584.

⁹⁶Opusc. anal., 1, 1773, 242; Comm. Arith., 2, p. 8.

⁹⁷De numeris amicabilebus, Comm. Arith., 2, 1849, 630; Opera postuma, 1, 1862, 88.

⁹⁸Tractatus de numerorum doctrina, Comm. Arith., 2, 514; Opera postuma, 1, 14-15.

⁹⁹Récréations math. et physiques par Ozanam, nouvelle éd. par M., Paris, 1, 1778, 1790, p. 33.

Engl. transl. by C. Hutton, London, 1803, p. 35.

Johann Philipp Gröson¹⁰⁰ made the same criticism of Ozanam⁷⁹ and noted that, if $2^n x$ is perfect and x is an odd prime,

$$1 + 2 + \dots + 2^n = 2^n x - x - 2x - \dots - 2^{n-1}x = x.$$

M. Fontana¹⁰¹ noted that the theorem that all perfect numbers are triangular is due to Maurolycus⁴¹ and not to T. Maier (cf. Kraft⁸⁵).

Thomas Taylor¹⁰² stated that only eight perfect numbers have been found so far [the 8 listed are those of Mersenne⁶⁰].

J. Struve¹⁰³ considered abundant numbers which are products abc of three distinct primes in ascending order; thus

$$\frac{ab+a+b+1}{ab-a-b-1} > c, \quad \frac{2}{1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{ab}} > c+1.$$

The case $a \geq 3$ is easily excluded, also $a=2$, $b \geq 5$ [except 2·5·7]. For $a=2$, $b=3$, c any prime > 3 , $6c$ is abundant. Next, $abcd$ is abundant if

$$\frac{2abc}{abc - (ab+ac+bc+a+b+c+1)} > d+1.$$

For $a=2$, $b=3$, $c=5$ or 7 , and for $a=2$, $b=5$, $c=7$, $abcd$ is abundant for any prime d [$> c$]. Of the numbers ≤ 1000 , 52 are abundant.

J. Westerberg¹⁰⁴ gave the factors of $2^n \pm 1$ for $n=1, \dots, 32$, and of $10^n \pm 1$, $n=1, \dots, 15$.

O. Terquem¹⁰⁵ listed $2^{41} - 1$ and $2^{47} - 1$ as primes.

L. Wantzel¹⁰⁶ proved the remark of Kraft⁸⁵ that if N_1 be the sum of the digits of a perfect number $N > 6$ [of Euclid's type], and N_2 the sum of the digits of N_1 , etc., a certain N_i is unity. Since $N \equiv 1 \pmod{9}$, each $N_i \equiv 1 \pmod{9}$, while the N_i 's decrease.

V. A. Lebesgue¹⁰⁷ stated that he had a proof that there is no odd perfect number with fewer than four distinct prime factors. For an even perfect number $2^\alpha y^\beta z^\gamma \dots$,

$$y^\beta z^\gamma \dots + \frac{y^\beta z^\gamma \dots}{2^{\alpha+1} - 1} = (1+y+\dots+y^\beta)(1+z+\dots+z^\gamma) \dots,$$

¹⁰⁰Enthüllte Zaubereyen und Geheimnisse der Arithmetik, erster Theil, Berlin, 1796, p. 85, and Zusatz (end of Theil I).

¹⁰¹Memorie dell' Istituto Nazionale Ital., mat., 2, pt. 1, 1808, 285-6.

¹⁰²The elements of a new arithmetical notation and of a new arithmetic of infinites, with an appendix... of perfect, amicable and other numbers no less remarkable than novel, London, 1823, 131.

¹⁰³Ueber die so genannten numeri abundantes oder die Ueberfluss mit sich führenden Zahlen, besonders im ersten Tausend unsrer Zahlen, Altona, 1827, 20 pp.

¹⁰⁴De factoribus numerorum compositorum dignoscendis, Disquisitio Acad. Carolina, Lundae, 1838. In the volume, Meditationum Math.... publice defendent C. J. D. Hill, Pt. II, 1831.

¹⁰⁵Nouv. Ann. Math., 3, 1844, 219 (cf. 553).

¹⁰⁶Ibid., p. 337.

¹⁰⁷Ibid., 552-3.

the impossibility of which is evident when the exponents β, γ, \dots are other than 1, 0, 0, \dots , a case giving Euclid's solution [cf. Desboves¹²⁷].

C. G. Reuschle¹⁰⁸ gave in his table C the exponent to which 2 belongs modulo p , for each prime $p < 5000$. Thus $2^n - 1$ has the factor 1399 for $n = 233$, the factor 2687 for $n = 79$, and 3391 for $n = 113$ [as stated explicitly by Le Lasseur^{119, 132}]; also 2351·4513 for $n = 47$, 1433 for $n = 179$, and 1913 for $n = 239$. In the addition (p. 22) to Table A, he gave the prime factors of $2^n - 1$ for various n 's to 156, 37 being the least n for which the decomposition is not given completely, while 41 is the least n for which no factor is known. For 34 errata in Table C, see Cunningham¹¹⁰ of Ch. VII.

F. Landry¹⁰⁹ gave a new proof that $2^{31} - 1$ is a prime.

Jean Plana¹¹⁰ gave (p. 130) the factorization into two primes:

$$2^{41} - 1 = 13367 \times 164511353.$$

His statement (p. 141) that $2^{53} - 1$ has no factor < 50033 was corrected by Landry¹¹³ (quoted by Lucas,¹¹⁹ p. 280) and Gérardin.¹⁷⁷

Giov. Nocco¹¹¹ showed that an odd perfect number has at least three distinct prime factors. For, if $a^m b^n$ is perfect,

$$2a^m = \frac{b^{n+1} - 1}{b - 1}, \quad b^n = \frac{a^{m+1} - 1}{a - 1},$$

whence

$$\frac{a}{2(b-1)} = \frac{a^{m+1}}{2(b-1)a^m} = \frac{(a-1)b^n + 1}{b^{n+1} - 1},$$

$$a + b(ab^n + 2b^{n-1} + 2) = 2 + b(2b^n + 2ab^{n-1}).$$

But the minimum values of a, b are 3, 5. Thus $b(a-2) > 2a-2$,

$$ab^n - 2b^n = b^{n-1} \cdot b(a-2) > b^{n-1}(2a-2), \quad ab^n + 2b^{n-1} > 2b^n + 2ab^{n-1},$$

contrary to the earlier equation. In attempting to prove that every even perfect number $2^m b^n c^r d^s \dots$ is of Euclid's type, he stated without proof that

$$2^{m+1} b^n c^r \dots = (2^{m+1} - 1)BC \dots, \quad B = \frac{b^{n+1} - 1}{b - 1}, \quad C = \frac{c^{r+1} - 1}{c - 1}, \dots$$

require that $2^{m+1} = B$, $b^n = 2^{m+1} - 1$, $d^s = C, \dots$ (the first two of which results yield Euclid's formula).

F. Landry¹¹² stated (p. 8) that he possessed the complete decomposition of $2^n \pm 1$ ($n \leq 64$) except for $2^{61} \pm 1$, $2^{64} + 1$, and gave (pp. 10-11) the factors of $2^{75} - 1$ and of $2^n + 1$ for $n = 65, 66, 69, 75, 90, 105$.

¹⁰⁸Mathematische Abhandlung, enthaltend neue Zahlentheoretische Tabellen sammt einer dieselben betreffenden Correspondenz mit dem verewigten C. G. J. Jacobi. Prog., Stuttgart, 1856, 61 pp. Described by Kummer, Jour. für Math., 53, 1857, 379.

¹⁰⁹Procédés nouveaux pour demontrer que le nombre 2147483647 est premier. Paris, 1859. Reprinted in Sphinx-Oedipe, Nancy, 1909, 6-9.

¹¹⁰Mem. Reale Ac. Sc. Torino, (2), 20, 1863, dated Nov. 20, 1859.

¹¹¹Alcune teorie su'numeri pari, impari, e perfetti, Lecce, 1863.

¹¹²Aux mathématiciens de toutes les parties du monde: communication sur la décomposition des nombres en leurs facteurs simples, Paris, 1867, 12 pp.

F. Landry¹¹³ soon published his table. It includes the entries (quoted by Lucas^{120, 122}):

$$2^{43} - 1 = 431 \cdot 9719 \cdot 2099863, \quad 2^{47} - 1 = 2351 \cdot 4513 \cdot 13264529, \\ 2^{53} - 1 = 6361 \cdot 69431 \cdot 20394401, \quad 2^{59} - 1 = 179951 \cdot 3203431780337,$$

the least factors of the first two of which had been given by Euler.^{83, 93} This table was republished by Lucas¹²³ (p. 239), who stated that only three entries remain in doubt: $2^{61} - 1$, $(2^{61} + 1)/3$, $2^{64} + 1$, each being conjectured a prime by Landry. The second was believed to be prime by Kraitchik.^{113a} Landry's factors of $2^n + 1$, for $28 \leq n \leq 64$ were quoted elsewhere.^{113b}

Jules Carvallo¹¹⁴ announced that he had a proof that there exists no odd perfect number. Without indication of proof, he stated that an odd perfect number must be a square and that the ratio of the sum of the divisors of an odd square to itself cannot be 2. The first statement was abandoned in his published erroneous proof,¹¹³ while the second follows at once from the fact that, when p is an odd prime, the sum of the $2n + 1$ divisors, each odd, of p^{2n} is odd.

E. Lucas¹¹⁵ stated that long calculations of his indicated that $2^{67} - 1$ and $2^{89} - 1$ are composite [cf. Cole,¹⁷³ Powers¹⁸⁵]. See Lucas²⁰ of Ch. XVII.

E. Lucas¹¹⁶ stated that $2^{31} - 1$ and $2^{127} - 1$ are primes.

E. Catalan¹¹⁶ remarked that, if we admit the last statement, and note that $2^2 - 1$, $2^3 - 1$, $2^7 - 1$ are primes, we may state empirically that, up to a certain limit, if $2^n - 1$ is a prime p , then $2^p - 1$ is a prime q , $2^q - 1$ is a prime, etc. [cf. Catalan¹³⁵].

G. de Longchamps¹¹⁷ suggested that the composition of $2^n \pm 1$ might be obtained by continued multiplications, made by simple displacements from right to left, of the primes written to the base 2.

E. Lucas¹¹⁸ verified once only that $2^{127} - 1$, a number of 39 digits, is a prime. The method will be given in Ch. XVII, where are given various results relating indirectly to perfect numbers. He stated (p. 162) that he had the plan of a mechanism which will permit one to decide almost instantaneously whether the assertions of Mersenne and Plana that $2^n - 1$ is a prime for $n = 53, 67, 127, 257$ are correct. The inclusion of $n = 53$ is an error of citation. He tabulated prime factors of $2^n - 1$ for $n \leq 40$.

E. Lucas¹¹⁹ gave a table of primes with 12 to 16 digits occurring as a factor in $2^n - 1$ for $n = 49, 59, 65, 69, 87$, and in $2^n + 1$ for $n = 43, 47, 49, 53, 69, 72, 75, 86, 94, 98, 99, 135$, and several even values of $n > 100$. The

¹¹³Décomposition des nombres $2^n \pm 1$ en leurs facteurs premiers de $n = 1$ à $n = 64$, moins quatre, Paris, 1869, 8 pp.

^{113a}Sphinx-Oedipe, 1911, 70, 95.

^{113b}L'intermédiaire des math., 9, 1902, 186.

¹¹⁴Comptes Rendus Paris, 81, 1875, 73-75.

¹¹⁵Sur la théorie des nombres premiers, Turin, 1876, p. 11; Théorie des nombres, 1891, 376.

¹¹⁶Nouv. Corresp. Math., 2, 1876, 96.

¹¹⁷Comptes Rendus Paris, 85, 1877, 950-2.

¹¹⁸Bull. Bibl. Storia Sc. Mat. e Fis., 10, 1877, 152 (278-287). Lucas^{18, 28} of Ch. XVII.

¹¹⁹Atti R. Ac. Sc. Torino, 13, 1877-8, 279.

verification of the primality was made by H. Le Lasseur. To the latter is attributed (p. 283) the factorization of $2^n - 1$ for $n = 73, 79, 113$. These had been given without reference by Lucas.¹²⁰

E. Lucas¹²¹ proposed as a problem the proof that if $8q + 7$ is a prime, $2^{4q+3} - 1$ is not.

E. Lucas¹²² stated as new the assertion of Euler⁸³ that if $4m - 1$ and $8m - 1$ are primes, the latter divides $A = 2^{4m-1} - 1$.

E. Lucas¹²³ proved the related fact that if $8m - 1$ is a prime, it divides A . For, by Fermat's theorem, it divides $2^{8m-2} - 1$ and hence divides A or $2^{4m-1} + 1$. That the prime $8m - 1$ divides A and not the latter, follows from Euler's criterion that $2^{(p-1)/2} - 1$ is divisible by the prime p if 2 is a quadratic residue of p , which is the case if $p = 8m \pm 1$. No reference was made to Euler, who gave the first seven primes $4m - 1$ for which $8m - 1$ is a prime. Lucas gave the new cases 251, 359, 419, 431, 443, 491. Lucas¹²⁴ elsewhere stated that the theorem results from the law of reciprocity for quadratic residues, again without citing Euler. Later, Lucas¹²⁵ again expressly claimed the theorem as his own discovery.

T. Pepin¹²⁶ noted that if p is a prime and $q = 2^p - 1$ is a quadratic non-residue of a prime $4n + 1 = a^2 + b^2$, then q is a prime if and only if $(a - bi)/(a + bi)$ is a quadratic non-residue of q .

A. Desboves¹²⁷ amplified the proof by Lebesgue¹⁰⁷ that every even perfect number is of Euclid's type by noting that the fractional expression in Lebesgue's equation must be an integer which divides $y^\beta z^\gamma \dots$ and hence is a term of the expansion of the second member. Hence this expansion produces only the two terms in the left member, so that $(\beta + 1)(\gamma + 1) \dots = 2$. Thus one of the exponents, say β , is unity and the others are zero. The same proof has been given by Lucas¹²³ (pp. 234-5) and *Théorie des Nombres*, 1891, p. 375. Desboves (p. 490, exs. 31-33) stated that no odd perfect number is divisible by only 2 or 3 distinct primes, and that in an odd perfect number which is divisible by just n distinct primes the least prime is less than 2^n .

F. J. E. Lionnet¹²⁸ amplified Euler's⁹⁸ proof about odd perfect numbers.

F. Landry¹²⁹ stated that $2^{61} \pm 1$ are the only cases in doubt in his table.¹¹³

Moret-Blanc¹³⁰ gave another proof that $2^{31} - 1$ is a prime.

¹²⁰Assoc. franç. avanc. sc., 6, 1877, 165.

¹²¹Nouv. Corresp. Math., 3, 1877, 433.

¹²²Mess. Math., 7, 1877-8, 186. Also, Lucas.¹¹⁹

¹²³Amer. Jour. Math., 1, 1878, 236.

¹²⁴Bull. Bibl. Storia Sc. Mat. e Fis., 11, 1878, 792. The results of this paper will be cited in Ch. XVI.

¹²⁵Récréations math., ed. 2, 1891, 1, p. 236.

¹²⁶Comptes Rendus Paris, 86, 1878, 307-310.

¹²⁷Questions d'algèbre élémentaire, ed. 2, Paris, 1878, 487-8.

¹²⁸Nouv. Ann. Math., (2), 18, 1879, 306.

¹²⁹Bull. Bibl. Storia Sc. Mat., 13, 1880, 470, letter to C. Henry.

¹³⁰Nouv. Ann. Math., (2), 20, 1881, 263. Quoted, with Lucas' proof, *Sphinx-Oedipe*, 4, 1909, 9-12.

H. LeLasseur found after¹³¹ 1878 and apparently just before¹³² 1882 that $2^n - 1$ has the prime factor 11447 if $n = 97$, 15193 if $n = 211$, 18121 if $n = 151$, 18287 if $n = 223$, and that there is no divisor < 30000 of $2^n - 1$ for the 24 prime values of n , $n \leq 257$, which remain in doubt, viz. [cf. Lucas¹³⁶],

61, 67, 71, 89, 101, 103, 107, 109, 127, 137, 139, 149,
157, 163, 167, 173, 181, 193, 197, 199, 227, 229, 241, 257.

J. Carvallo¹³³ attempted again¹¹⁴ to prove the non-existence of odd perfect numbers $y^n z^p \dots u^r$, where y, \dots, u are distinct odd primes. He began by noting that one and only one of the exponents n, \dots, r is odd [Euler⁹⁸]. Let $y < z < \dots < u$, and call their number μ . From the definition of a perfect number,

$$\frac{y-1}{y-1} \dots \frac{u-1}{u-1} = 2, \quad \frac{y}{y-1} \dots \frac{u}{u-1} > 2.$$

The fractions in this inequality form a decreasing series. Hence

$$\left(\frac{y}{y-1}\right)^\mu > 2, \quad y < \frac{2^{1/\mu}}{2^{1/\mu}-1}, \quad k \cdot \frac{u}{u-1} > 2, \quad k \equiv \left(\frac{y}{y-1}\right)^{\mu-1}.$$

Thus $u(2-k) < 2$. By a *petitio principii* (the division by $2-k$, not known to be positive), it was concluded (p. 10) that

$$u < \frac{2}{2-k}, \quad k < 2, \quad y > \frac{2^{1/(\mu-1)}}{2^{1/(\mu-1)}-1}.$$

[This error, repeated on p. 15, was noted by P. Mansion.¹³⁴] For a given μ , there is at most one prime between the two limits (of difference < 2) for y . A superior limit is found for z as a function of y . An incomplete computation is made to show that, if $\mu > 8$, $z < y + 1$.

It is shown (p. 7) that an odd perfect number has a prime factor greater than the prime factor w entering to an odd power, since $w+1$ divides the sum of the divisors. In a table (p. 30) of the first ten perfect numbers, $2^{29} - 1$ and $2^{41} - 1$ are entered as primes [contrary to Euler⁹³ and Plana¹¹⁰].

E. Catalan¹³⁵ stated that $2^p - 1$ is a prime if p is a prime of the form $2^\lambda - 1$. If correct this would imply that $2^{127} - 1$ is a prime [cf. Catalan¹¹⁶].

E. Lucas¹³⁶ repeated the remark of LeLasseur¹³² on the 24 prime values of $n \leq 257$ for which the composition of $2^n - 1$ is in doubt. According to a

¹³¹Since these four values of n are included in the list by Lucas¹²⁴ of the 28 values of $n \leq 257$ for which the composition of $2^n - 1$ is unknown. Cf. Lucas¹²³, p. 236.

¹³²Lucas, *Récréations math.*, 1, 1882, 241; 2, 1883, 230. Later, Lucas¹²⁵ credited LeLasseur with these four cases as well as $n = 73$ [Euler⁹³] and $n = 79, 113, 233$ [cf. Reuschle¹⁰⁸]. The last four cases were given by Lucas¹²⁴, while the last three do not occur in the table (Lucas¹²⁴, pp. 788-9) by LeLasseur of the proper divisors of $2^n - 1$ for each odd n , $n < 79$, and for a few larger composite n 's. The last three were given also by Lucas¹²³ (p. 236) without reference.

¹³³*Théorie des nombres parfaits*, par M. Jules Carvallo, Paris, 1883, 32 pp.

¹³⁴*Mathesis*, 6, 1886, 147.

¹³⁵*Mélanges Math.*, Bruxelles, 1, 1885, 376.

¹³⁶*Mathesis*, 6, 1886, 146.

communication from Pellet, $2^n - 1$ is divisible by $6n + 1$ if n and $6n + 1$ are primes such that $6n + 1 = 4L^2 + 27M^2$ [provided* $n \equiv 1 \pmod{4}$, i. e., L is odd].

M. A. Stern¹³⁷ amplified Euler's⁹⁸ proof concerning odd perfect numbers.

E. Lucas¹³⁸ repeated the statement [Desboves¹²⁷] that an odd perfect number must contain at least four distinct primes.

G. Valentin¹³⁹ gave a table, computed in 1872, showing factors of $2^n - 1$ for $n = 79, 113, 233$, etc., but not the new cases of LeLasseur.¹³²

The primality of $N = 2^{61} - 1$, a number of 19 digits, considered composite by Mersenne and prime by Landry, was established by J. Pervušin¹⁴⁰ and P. Seelhoff¹⁴¹ independently. The latter claimed to verify that there is no factor $< N^{1/3}$ of the form $8n + 7$, abbreviating the work by use of various numbers of which N is a quadratic residue; thus N is a prime or the product of two primes. Since $N = 2(2^{30})^2 - 1$, 2 is a quadratic residue of any prime factor of N , so that the factor is $8n \pm 1$. It was verified that $3^\beta \equiv 1 \pmod{N}$, where $\beta = (N - 1)/9$. If $N = fF$, where F is the prime factor $8n + 1$, then $3^\beta \equiv 1 \pmod{F}$ and, by Fermat's theorem, $3^{F-1} \equiv 1 \pmod{F}$. It is stated without proof that one of the exponents β and $F - 1$ divides the other. Cole¹⁷³ regarded the proof as unsatisfactory.

Seelhoff proved that a perfect number of the form $p^\pi r^\rho$ is of Euclid's type if p and r are primes and $p < r$. The condition is

$$p^\pi = \frac{r^{\rho+1} - 1}{r^{\rho+1}(2-p) - 2r^\rho(1-p) - p}.$$

If $p > 2$, the denominator is negative. Hence $p = 2$ and

$$2^\pi = \frac{r^{\rho+1} - 1}{2r^\rho - 2}, \quad 2^{\pi+1} = r + \frac{r-1}{r^\rho - 1}, \quad \rho = 1, \quad r = 2^{\pi+1} - 1.$$

His statements (p. 177) about the factors of $2^n - 1$, $n = 37, 47, 53, 59$, were corrected by him (*ibid.*, p. 320) to accord with Landry.¹¹³

P. Seelhoff¹⁴² obtained the known factors of these $2^n - 1$ and proved that $2^{31} - 1$ is a prime, by use of his method of quadratic residues.

H. Novarese¹⁴³ proved that every perfect number of Euclid's type ends in 6 or 28, and that each one > 6 is of the form $9k + 1$.

Jules Hudelot¹⁴⁴ verified in 54 hours that $2^{61} - 1$ is a prime by use of the test by Lucas, *Récréations math.*, 2, 1883, 233.

*Correction by Kraitchik, *Sphinx-Oedipe*, 6, 1911, 73; Pellet, 7, 1912, 15.

¹³⁷Mathesis, 6, 1886, p. 248.

¹³⁸*Ibid.*, p. 250.

¹³⁹Archiv Math. Phys., (2), 4, 1886, 100-3.

¹⁴⁰Bull. Acad. Sc. St. Pétersb., (3), 31, 1887, p. 532; Mélanges math. astr. ac. St. Pétersb., 6, 1881-8, 553; communicated Nov. 1883.

¹⁴¹Zeitschr. Math. Phys., 31, 1886, 174-8.

¹⁴²Archiv Math. Phys., (2), 2, 1885, 327; 5, 1887, 221-3 (misprint for $n = 41$).

¹⁴³Jornal de ciencias math. e astr., 8, 1887, 11-14. [Servais¹⁴⁵.]

¹⁴⁴Mathesis, 7, 1887, 46. *Sphinx-Oedipe*, 1909, 16.

Cl. Servais¹⁴⁵ republished the proofs by Novarese¹⁴³ and proved that $a^m b^n$ is not perfect if a and b are odd primes. For, by the equations [Nocco¹¹¹]

$$a^{m+1} - 1 = b^n(a-1), \quad b^{n+1} - 1 = 2a^m(b-1),$$

we obtain, by subtraction,

$$(2a^m - b^n)(a+b-1) = a^{m+1}.$$

Thus $2a^m > b^n$. Since $a \geq 3$, $a^{m+1} \geq 3a^m > a^m + b^n > a + b - 1$. He next proved that, if an odd perfect number is divisible by only three distinct primes a , b , c , two of them are 3 and 5, since [as by Carvallo¹³³]

$$\left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \left(1 - \frac{1}{c}\right) < \frac{1}{2}.$$

Taking $a=3$, $b=5$, we have $c < 16$, whence $c=7$, 11, or 13. He quoted from a letter from Catalan that the sum of the reciprocals of the divisors of a perfect number equals 2.

E. Cesàro¹⁴⁶ proved that in an odd perfect number containing n distinct prime factors, the least prime factor is $\leq n\sqrt{2}$.

Cl. Servais¹⁴⁷ showed that it does not exceed n since, if $a < b < c < \dots$,

$$\frac{b}{b-1} < \frac{a+1}{a}, \quad \frac{c}{c-1} < \frac{a+2}{a+1}, \dots$$

$$2 < \frac{a}{a-1} \cdot \frac{b}{b-1} \dots < \frac{a}{a-1} \cdot \frac{a+1}{a} \cdot \frac{a+2}{a+1} \dots \frac{a+n-1}{a+n-2},$$

whence $2(a-1) < a+n-1$, $a < n+1$. If l is the $(m-1)$ th prime factor and s is the m th, and if

$$\frac{a}{a-1} \cdot \frac{b}{b-1} \dots \frac{l}{l-1} \leq L < 2,$$

then

$$L \cdot \frac{s}{s-1} \cdot \frac{s+1}{s} \dots \frac{s+n-m}{s+n-m+1} > 2, \quad s < \frac{L(n-m)+2}{2-L}.$$

J. J. Sylvester¹⁴⁸ reproduced Euler's⁹⁷ proof that every even perfect number is of Euclid's type. From the fact that $\frac{3}{2} \cdot \frac{5}{4} < 2$, he concluded that there is no odd perfect number $a^m b^n$. For the case of three prime factors he obtained the result of Servais¹⁴⁵ in the same manner. He proved that no odd perfect number is divisible by 105 and stated that there is none with fewer than six distinct prime factors.

Sylvester¹⁴⁹ and Servais¹⁵⁰ gave complete proofs that there exists no odd perfect number with only three distinct prime factors.

¹⁴⁵Mathesis, 7, 1887, 228-230.

¹⁴⁶*Ibid.*, 245-6.

¹⁴⁷Mathesis, 8, 1888, 92-3.

¹⁴⁸Nature, 37, Dec. 15, 1887, 152 (minor correction, p. 179); Coll. Math. Papers, 4, 1912, 588.

¹⁴⁹Comptes Rendus Paris, 106, 1888, 403-5 (correction, p. 641); reproduced with notes by P.

Mansion, Mathesis, 8, 1888, 57-61. Sylvester's Coll. Math. Papers, 4, 1912, 604, 615.

¹⁵⁰Mathesis, 8, 1888, 135.

Sylvester¹⁵¹ proved there is no odd perfect number not divisible by 3 with fewer than eight distinct prime factors.

Sylvester¹⁵² proved there is no odd perfect number with four distinct prime factors.

Sylvester¹⁵³ spoke of the question of the non-existence of odd perfect numbers as a "problem of the ages comparable in difficulty to that which previously to the labors of Hermite and Lindemann environed the subject of the quadrature of the circle." He gave a theorem useful for the investigation of this question: For r an integer other than 1 or -1 , the sum $1+r+r^2+\dots+r^{p-1}$ contains at least as many distinct prime factors as p contains divisors >1 , with a possible reduction by one in the number of prime factors when $r=-2$, p even, and when $r=2$, p divisible by 6.

E. Catalan¹⁵⁴ proved that if an odd perfect number is not divisible by 3, 5, or 7, it has at least 26 distinct prime factors and thus has at least 45 digits. In fact, the usual inequality gives

$$\frac{10}{11} \cdot \frac{12}{13} \cdots \frac{l-1}{l} < \frac{1}{2}, \quad P(l) \equiv \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdots \frac{l-1}{l} < \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} < 0.2285.$$

By Legendre's table IX, *Théorie des nombres*, ed. 2, 1808; ed. 3, 1830, of the values of $P(w)$ up to $w=1229$, we see that $l \geq 127$. But 127 is the 27th prime >7 .

R. W. D. Christie¹⁵⁵ erroneously considered $2^{41}-1$ and $2^{47}-1$ as primes.

E. Lucas¹⁵⁶ proved that every even perfect number, aside from 6 and 496, ends with 16, 28, 36, 56, or 76; any one except 28 is of the form $7k \pm 1$; any one except 6 has the remainder 1, 2, 3, or 8 when divided by 13, etc.

E. Lucas¹⁵⁷ reproduced his¹⁵⁶ proofs and the proof by Euler,⁹⁸ and gave (p. 375) a list of known factorizations of 2^n-1 .

Genaille¹⁵⁸ stated that his machine "piano arithmétique" gives a practical means of applying in a few hours the test by Lucas (*ibid.*, 5, 1876, 61) for the primality of 2^n-1 .

J. Fitz-Patrick and G. Chevrel¹⁵⁹ stated that $2^{28}(2^{29}-1)$ is perfect.

E. Fauquembergue¹⁶⁰ found that $2^{67}-1$ is composite by a process not yielding its factors [cf. Mersenne,⁶⁰ Lucas,¹¹⁵ Cole¹⁷³].

A. Cunningham¹⁶¹ called 2^p-1 a Lucassian if p is a prime of the form $4k+3$ such that also $2p+1$ is a prime, stating that Lucas¹²³ had proved that 2^p-1 has the factor $2p+1$. Cunningham listed all such primes $p < 2500$

¹⁵¹*Comptes Rendus Paris*, 106, 1888, 448-450; Coll. M. Papers, IV, 609-610.

¹⁵²*Ibid.*, 522-6; Coll. M. Papers, IV, 611-4.

¹⁵³*Nature*, 37, 1888, 417-8; Coll. M. Papers, IV, 625-9.

¹⁵⁴*Mathesis*, 8, 1888, 112-3. *Mém. soc. sc. Liège*, (2), 15, 1888, 205-7 (*Mélanges math.*, III).

¹⁵⁵*Math. Quest. Educat. Times*, 48, 1888, p. xxxvi, 183; 49, p. 85.

¹⁵⁶*Mathesis*, 10, 1890, 74-76.

¹⁵⁷*Théorie des nombres*, 1891, 424-5.

¹⁵⁸*Assoc. franç. avanc. sc.*, 20, I, 1891, 159.

¹⁵⁹*Exercices d'Arith.*, Paris, 1893, 363.

¹⁶⁰*L'intermédiaire des math.*, 1, 1894, 148; 1915, 105, for representations by u^2+67v^2 .

¹⁶¹*British Assoc. Reports*, 1894, 563.

and considered it probable that primes of the forms $2^x \pm 1$, $2^x \pm 3$ (if not yielding Lucassians) generally yield prime values of $2^p - 1$, and that no other primes will. All known and conjectured primes $2^p - 1$, with p prime, fall under this rule.

In a letter to Tannery,¹⁶² Lucas stated that Mersenne^{60,61} implied that a necessary and sufficient condition that $2^p - 1$ be a prime is that p be a prime of one of the forms $2^{2n} + 1$, $2^{2n} \pm 3$, $2^{2n+1} - 1$. Tannery expressed his belief that the theorem was empirical and due to Frenicle, rather than to Fermat, and noted that the sufficient condition would be false if $2^{67} - 1$ is composite [as is the case, Fauquembergue¹⁶⁰].

Goulard and Tannery¹⁶³ made minor remarks on the subject of the last two papers.

A. Cunningham¹⁶⁴ found that $2^{197} - 1$ has the factor 7487. This contradicts LeLasseur's¹³² statement on divisors < 30000 of Mersenne's numbers.

A. Cunningham¹⁶⁵ found 13 new cases (317, 337, 547, 937, . . .) in which $2^q - 1$ is composite, and stated that for the 22 outstanding primes $q \leq 257$ [above list¹³² except 61, 197] $2^q - 1$ has no divisor $< 50,000$ (error as to $q = 181$, see Woodall¹⁸⁴). The factors obtained in the mentioned 13 cases were found after much labor by the indirect method of Bickmore,¹⁶⁶ who gave the factors 1913 and 5737 of $2^{239} - 1$.

A. Cunningham¹⁶⁷ gave a factor of $2^q - 1$ for $q = 397, 1801, 1367, 5011$ and for five larger primes q .

C. Bourlet¹⁶⁸ proved that the sum of the reciprocals of all the divisors d_i of a perfect number n equals 2 [Catalan¹⁴⁵], by noting that n/d_i ranges with d_i over the divisors of n , so that $2n = \sum n/d_i$. The same proof occurs in Il Pitagora, Palermo, 16, 1909-10, 6-7.

M. Stuyvaert¹⁶⁹ remarked that an odd perfect number, if it exists, is a sum of two squares since it is of the form pk^2 , where p is a prime $4n + 1$ [Frenicle,⁶⁴ Euler⁹⁸].

T. Pepin¹⁷⁰ proved that an odd perfect number relatively prime to 3·7, 3·5 or 3·5·7 contains at least 11, 14 or 19 distinct prime factors, respectively, and can not have the form $6k + 5$.

F. J. Studnička¹⁷¹ called $E_p = 2^{p-1}(2^p - 1)$ an Euclidean number if $2^p - 1$ is a prime. The product of all the divisors $< E_p$ of E_p is E_p^{p-1} . When E_p is written in the diadic system (base 2), it has $2p - 1$ digits, the first p of which are unity and the last $p - 1$ are zero.

¹⁶²L'intermédiaire des math., 2, 1895, 317.

¹⁶³Ibid., 3, 1896, 115, 188, 281.

¹⁶⁴Nature, 51, 1894-5, 533; Proc. Lond. Math. Soc., 26, 1895, 261; Math. Quest. Educat. Times, 5, 1904, 108, last footnote.

¹⁶⁵British Assoc. Reports, 1895, 614.

¹⁶⁶On the numerical factors of $a^n - 1$, Messenger Math., 25, 1895-6, 1-44; 26, 1896-7, 1-38. French transl. by Fitz-Patrick, Sphinx-Oedipe, 1912, 129-144, 155-160.

¹⁶⁷Proc. London Math. Soc., 27, 1895-6, 111.

¹⁶⁸Nouv. Ann. Math., (3), 15, 1896, 299.

¹⁶⁹Mathesis, (2), 6, 1896, 132.

¹⁷⁰Memoire Accad. Pont. Nuovi Lincei, 13, 1897, 345-420.

¹⁷¹Sitzungsber. Böhm. Gesell., Prag, 1899, math. nat., No. 30.

Mario Lazzarini¹⁷² attempted to prove that there is no odd perfect number $a^\alpha b^\beta c^\gamma$, but made the error of thinking that a is relatively prime to $b^\beta + \dots + b + 1$. He attempted to show that $p = 2^a - 1$ is a prime if and only if p divides $N = 3^k + 1$, where $k = 2^{a-1} - 1$ [false for $a = 2$, since $p = 3$, $N = 4$]. He restricted his argument to the case a odd, whence $p \equiv 1 \pmod{3}$. Then, if p is a prime, -3 is a quadratic residue of p , so that $(-3)^{(p-1)/2} \equiv 1 \pmod{p}$, whence p divides N . Conversely, when this congruence holds, he concluded falsely that $z^2 \equiv -3 \pmod{p}$ has two and only two roots, so that p is expressible in a single way as a sum of a square and the triple of a square and hence is prime. To show the error, let $p = ab$, where $a = 23$, $b = 3851$ are primes; then

$$(-3)^{11} + 1 = -2ab, \quad (-3)^{\frac{a-1}{2}} \equiv -1 \pmod{b}, \quad (-3)^{\frac{b-1}{2}} \equiv (-3)^{11 \cdot 175} \equiv -1 \pmod{a},$$

whence $(-3)^{(p-1)/2} \equiv 1 \pmod{p}$. Cipolla remarked (p. 288) that we may deduce from a result of Lucas¹²⁰ that p is a prime if it divides N without dividing $3^\delta + 1$ for any divisor δ of $p = 2^{a-1} - 1$.

F. N. Cole¹⁷³ found that $2^{67} - 1$ is the product of the two primes 193707721, 761838257287. In the footnote to p. 136, he criticized the proof by Seelhoff¹⁴¹ of the primality of $N = 2^{61} - 1$ and stated he had verified that N is prime by an actual computation of a series of primes of which N is a quadratic residue.

R. D. Carmichael¹⁷⁴ proved that any even perfect number $2^a p_2^{a_2} \dots p_n^{a_n}$ is of Euclid's type. Write d for $2^{a+1} - 1$. Then, as usual,

$$\frac{2^{a+1}}{d} = \prod \frac{(p_i^{a_i} + \dots + p_i + 1)}{p_i^{a_i}}, \quad 1 + \frac{1}{d} \geq \prod \left(1 + \frac{1}{p_i}\right).$$

If $n > 2$, p_i is less than d , being an aliquot divisor of it, so that $1 + 1/p_i$ exceeds the left member of the inequality. Hence $n = 2$, $p_2 = d$.

A. Cunningham¹⁷⁵ gave the residues of $k = 2^{2^n}$, 2^k , etc., modulo $2^a - 1$ for primes $q \leq 101$.

A. Turčaninov¹⁷⁶ (Turtschaninov) proved that an odd perfect number has at least four distinct prime factors and exceeds 2000000.

A. Gérardin¹⁷⁷ noted the error by Plana.¹¹⁰

A. Gérardin¹⁷⁸ stated the empirical laws: If n is a prime of the form $24x + 11$ and if $2^n - 1$ is composite, the least factor is of the form $24y + 23$

¹⁷²Periodico di mat. insegn. sec., 18, 1903, 203; criticized by C. Ciamberlini, p. 283, and by M. Cipolla, p. 285.

¹⁷³Bull. Amer. Math. Soc., 10, 1903-4, 134-7. French transl., Sphinx-Oedipe, 1910, 122-4. Cf. Fauquembergue.¹⁶⁰

¹⁷⁴Annals of Math., (2), 8, 1906-7, 149.

¹⁷⁵Proc. London Math. Soc., (2), 5, 1907, 259 [250].

¹⁷⁶Věst. opytn. fiziki (Spaczkinskis Bote), Odessa, 1908, No. 461 (pp. 106-113), No. 463 (162-3), No. 465-6 (213-9), No. 470 (314-8). In Russian. Cf. Bourlet.¹⁶⁸

¹⁷⁷L'intermédiaire des math., 15, 1908, 230-1.

¹⁷⁸Sphinx-Oedipe, Nancy, 3, 1908-9, 113-123; Assoc. franç. avanc. sc., 1909, 145-156. In *Wiskundig Tijdschrift*, 10, 1913, 61, he added that in the remaining three cases < 257 , $n = 107$, 167, 227, the least divisor (necessarily > 1 million) is respectively 5136 $y + 2783$, 8016 $y + 335$, 10896 $y + 5903$.

(e. g., $n = 11, 59, 83, 131, 179, 251$). If n is a prime $24x+23$ and 2^n-1 is composite, the least factor is of the form $48y+47$ (e. g., $n=47$, $y=48$, factor 2351; $n=23, 71, 191, 239$). Gérardin¹⁷⁹ gave tables of the possible, but (unverified, factors of 2^n-1 , $n < 257$).

A. Cunningham¹⁸⁰ gave the factor 150287 of $2^{163}-1$.

A. Cunningham¹⁸¹ found the factor 228479 of $2^{71}-1$.

T. M. Putnam¹⁸² proved that not all of the r distinct prime factors of a perfect number exceed $1+r/\log_e 2$ and hence do not all equal or exceed $1+3r/2$.

L. E. Dickson¹⁸³ gave an immediate proof that every even perfect number is of Euclid's type. Let $2^n q$ be perfect, where q is odd and $n > 0$. Then $(2^{n+1}-1)s = 2^{n+1}q$, where s is the sum of all the divisors of q . Thus $s = q+d$, where $d = q/(2^{n+1}-1)$. Hence d is an integral divisor of q , so that q and d are the only divisors of q . Hence $d=1$ and q is a prime.

H. J. Woodall¹⁸⁴ obtained the factor 43441 of $2^{181}-1$.

R. E. Powers¹⁸⁵ verified that $2^{89}-1$ is a prime by use of Lucas' test on the series 4, 14, 194, . . . H. Tarry¹⁸⁶ made an incomplete examination. E. Fauquembergue¹⁸⁷ proved that $2^{89}-1$ is a prime by writing the residues of that series to base 2.

A. Cunningham¹⁸⁸ noted that 2^q-1 is composite for three primes of 8 digits. On the proof-sheets of this history, he noted that the first two should be

$$q = 67108493, \quad p = 134216987; \quad q = 67108913, \quad p = 134217827.$$

A Gérardin^{188a} observed that $2^{2n+1}-1 = F^2 - 2G^2$, $F = 2^{n+1} \pm 1 = 2m+1$, $G = 2^n \pm 1$, $G^2 = m^2 + (m+1)^2 - (2^n)^2$.

H. Tarry^{188b} verified for the known composite numbers 2^p-1 , where p is a prime, that, if a is the least factor, 2^a-1 is composite.

A. Gérardin added empirically that, if p is any number and a any divisor of 2^p-1 , $a = 8m \pm 1$ not being of the form 2^n-1 then 2^a-1 is composite.

A. Cunningham¹⁸⁹ noted that, if q is a prime,

$$M_q = 2^q - 1 = T^2 - 2(qu)^2 = (qt)^2 - 2U^2.$$

If M_q is a prime it can be expressed in the forms $A^2 + 3B^2 = G^2 + 6H^2$, and in one or the other of the pairs of forms $t^2 \pm au^2$ ($a = 7, 14, 21, 42$). He discussed M_q to the base 2.

¹⁷⁹Sphinx-Oedipe, 3, 1908-9, 118-120, 161-5, 177-182; 4, 1909, 1-5, 158, 168; 1910, 149, 166.

¹⁸⁰Proc. London Math. Soc., (2), 6, 1908, p. xxii.

¹⁸¹L'intermédiaire des math., 16, 1909, 252; Sphinx-Oedipe, 4, 1909, 4e Trimestre, 36-7.

¹⁸²Amer. Math. Monthly, 17, 1910, 167.

¹⁸³Ibid., 18, 1911, 109.

¹⁸⁴Bull. Amer. Math. Soc., 16, 1910-11, 540 (July, 1911). Proc. London Math. Soc., (2), 9, 1911, p. xvi. Mem. and Proc. Manchester Literary and Phil. Soc., 56, 1911-12, No. 1, 5 pp. Sphinx-Oedipe, 1911, 92. Verification by J. Hammond, Math. Quest. Solutions, 2, 1916, 30-2.

¹⁸⁵Bull. Amer. Math. Soc., 18, 1911-12, 162 (report of meeting Oct., 1911). Amer. Math. Monthly, 18, 1911, 195. Sphinx-Oedipe, Feb., 1912, 17-20.

¹⁸⁶Sphinx-Oedipe, Dec., 1911, p. 192; 1912, 15. (Proc. London Math. Soc., (2), 10, 1912, Records of Meetings, 1911-12, p. ii.)

¹⁸⁷Ibid., 1912, 20-22.

¹⁸⁸Messenger Math., 41, 1911, 4.

^{188a}Bull. Soc. Philomatiques de Paris, (10), 3, 1911, 221. ^{188b}Sphinx-Oedipe, 6, 1911, 174 186, 192.

¹⁸⁹Math. Quest. Educ. Times, (2), 19, 1911, 81-2; 20, 1911, 90-1, 105-6; 21, 1912, 58-9, 73.

A. Cunningham¹⁹⁰ found the factor 730753 of $2^{173}-1$.

V. Ramesam¹⁹¹ verified that the quotient of $2^{71}-1$ by the factor 228479 [Cunningham¹⁸¹] is the product of the primes 48544121 and 212885833.

A. Aubry¹⁹² stated erroneously that "Mersenne affirmed that 2^n-1 is a prime, for $n \leq 257$, only for $n=1, 2, 3, 4, 8, 10, 12, 29, 61, 67, 127, 257$ (which has now been almost proved); this proposition seems to be due to Frenicle.⁵⁷" What Mersenne⁶⁰ actually stated was that the first 8 perfect numbers occur at the lines marked 1, 2, 3, 4, 8, etc., in the table by Bungus.

A. Cunningham^{192a} noted that M_{113} , M_{151} , M_{251} have the further factors 23279-65993, 55871, 54217, respectively. Cf. Reuschle¹⁰⁸, Lucas¹²³.

A. Gérardin^{192b} noted that there is no divisor < 1000000 of the composite Mersenne numbers not already factored. Let d denote the least divisor of 2^q-1 , q a prime ≤ 257 . If $q=60u+43$, then $d \equiv 47 \pmod{96}$, except for the cases given by Euler's⁸³ theorem (verified for 43, 163, 223). If $q=40u+33$, $d \equiv 7 \pmod{24}$, verified for 73, 113, 233. If $q=30m+1$, $d \equiv 1 \pmod{24}$, verified for 31, 61, 151, 181, 211.

E. Fauquembergue^{192c} proved that $2^{101}-1$ is composite by means of Lucas' test with 4, 14, 194, . . . , written to base 2 (Ch. XVII).

L. E. Dickson¹⁹³ called a non-deficient number *primitive* if it is not a multiple of a smaller non-deficient number, and proved that there is only a finite number of primitive non-deficient numbers having a given number of distinct odd prime factors and a given number of factors 2. As a corollary, there is not an infinitude of odd perfect numbers with any given number of distinct prime factors. There is no odd abundant number with fewer than three distinct prime factors; the primitive ones with three are

$$3^3 \cdot 5 \cdot 7, \quad 3^2 \cdot 5^2 \cdot 7, \quad 3^2 \cdot 5 \cdot 7^2, \quad 3^3 \cdot 5^2 \cdot 11, \quad 3^5 \cdot 5^2 \cdot 13, \quad 3^4 \cdot 5^3 \cdot 13, \quad 3^4 \cdot 5^2 \cdot 13^2, \quad 3^3 \cdot 5^3 \cdot 13^2.$$

There is given a list of the numerous primitive odd abundant numbers with four distinct prime factors and lists of even non-deficient numbers of certain types. In particular, all primitive non-deficient numbers < 15000 are determined (23 odd and 78 even). In view of these lists, there is no odd perfect number with four or fewer distinct prime factors (cf. Sylvester¹⁴⁸⁻¹⁵³).

A. Cunningham¹⁹⁴ gave a summary of the known results on the composition of the 56 Mersenne numbers $M_q = 2^q - 1$, q a prime ≤ 257 . Of these, 12 have been proved prime: M_q , $q=1, 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 127$; while 29 of them have been proved composite. Thus only 15 remain in

¹⁹⁰British Assoc. Reports, 1912, 406-7. Sphinx-Oedipe, 7, 1912, 38 (1910, 170, that 730753 is a possible factor). Cf. Cunningham¹⁹⁴.

¹⁹¹Nature, 89, 1912, p. 87; Sphinx-Oedipe, 1912, 38. Jour. of Indian Math. Soc., Madras, 4, 1912, 56.

¹⁹²Oeuvres de Fermat, 4, 1912, 250, note to p. 67.

^{192a}Mem. and Proc. Manchester Lit. and Phil. Soc., 56, 1911-2, No. 1.

^{192b}Sphinx-Oedipe, 7, 1912, numéro spécial, 15-16.

^{192c}Ibid., Nov., 1913, 176.

^{192d}Amer. Jour. Math., 35, 1913, 413-26.

¹⁹⁴Proc. Fifth International Congress, I, Cambridge, 1913, 384-6. Proc. London Math. Soc., (2), 11, 1913, Record of Meeting, Apr. 11, 1912, xxiv. British Assoc. Reports, 1911, 321. Math. Quest. Educat. Times, (2), 23, 1913, 76.

doubt: M_q , $q=101, 103, 107, 109, 137, 139, 149, 157, 167, 193, 199, 227, 229, 241, 257$. The last has no factor under one million, as verified by R. E. Powers.^{194a} No one of the other 14 has a factor under one million, as verified twice with the collaboration of A. Gérardin. Up to the present three errors have been found in Mersenne's assertion; M_{67} has been proved composite (Lucas,¹¹⁵ Cole¹⁷³), while M_{61} and M_{89} have been proved prime (Pervušin,¹⁴⁰ Seelhoff,¹⁴¹ Cole,¹⁷³ Powers¹⁸⁵). It is here announced that M_{173} has the factor 730753, found with the collaboration of A. Gérardin.

J. McDonnell¹⁹⁵ commented on a test by Lucas in 1878 for the primality of $2^n - 1$.

L. E. Dickson¹⁹⁶ gave a table of the even abundant numbers < 6232 .

R. Niewiadomski¹⁹⁷ noted that $2^{761} - 1$ has the factor 4567 and gave known factors of $2^n - 1$. He gave the formula

$$2^{6m+1} - 1 = (2^{2m} + 2^m - 1)^3 + (2^{2m} - 2^m - 1)^3 + 1.$$

G. Ricalde¹⁹⁸ gave relations between the primes p, q and least solutions of $2^{2n+1} - 1 = pq$, $a^2 - 2b^2 = p$, $c^2 - 2d^2 = q$.

R. E. Powers¹⁹⁹ proved that $2^{107} - 1$ is a prime by means of Lucas'³¹ test in Ch. XVII.

E. Fauquembergue²⁰⁰ proved that $2^p - 1$ is prime for $p=107$ and 127, composite for $p=101, 103, 109$.

T. E. Mason²⁰¹ described a mechanical device for applying Lucas'¹¹⁸ method for testing the primality of $2^{4x+3} - 1$.

R. E. Powers²⁰² proved that $2^{103} - 1$ and $2^{109} - 1$ are composite by means of Lucas' tests with 3, 7, 47, ... and 4, 14, 194, ... (Ch. XVII), respectively.

A. Gérardin²⁰³ gave a history of perfect numbers and noted that $2^p - 1$ can be factored if we find t such that $m = 2pt + 1$ is a prime not dividing $s = 1 + 2^p + 2^{2p} + \dots + 2^{(2t-1)p}$, since $2^{2pt} - 1 \equiv (2^p - 1)s \pmod{m}$. Or we may seek to express $2^p - 1$ in two ways in the form $x^2 - 2y^2$.

On tables of exponents to which 2 belongs, see Ch. VII, Cunningham and Woodall¹²⁸, Kraitchik.¹²⁵

ADDITIONAL PAPERS OF A MERELY EXPOSITORY CHARACTER.

E. Catalan, *Mathesis*, (1), 6, 1886, 100-1, 178.

W. W. Rouse Ball, *Messenger Math.*, 21, 1891-2, 34-40, 121.

Fontés (on Bovillus²⁰), *Mém. Ac. Sc. Toulouse*, (9), 6, 1894, 155-67.

J. Bezdiček, *Casopis Mat. a Fys.*, Prag, 25, 1896, 221-9.

Hultsch (on Iamblichus), *Nachr. Kgl. Sächs. Gesell.*, 1895-6.

H. Schubert, *Math. Mussestunden*, I, Leipzig, 1900, 100-5.

M. Nassò, *Revue de math. (Peano)*, 7, 1900-1, 52-53.

^{194a}*Sphinx-Oedipe*, 1913, 49-50.

¹⁹⁶*London Math. Soc.*, Records of Meeting, Dec., 1912, v-vi.

¹⁹⁶*Quart. Jour. Math.*, 44, 1913, 274-7.

¹⁹⁷*L'intermédiaire des math.*, 20, 1913, 78, 167.

¹⁹⁸*Ibid.*, 7-8, 149-150; cf. 140-1.

¹⁹⁹*Proc. London Math. Soc.*, (2), 13, 1914, Records of meetings, xxxix. *Bull. Amer. Math. Soc.*, 20, 1913-4, 531. *Sphinx-Oedipe*, 1914, 103-8.

²⁰⁰*Sphinx-Oedipe*, June, 1914, 85; *L'intermédiaire des math.*, 24, 1917, 33.

²⁰¹*Proc. Indiana Acad. Science*, 1914, 429-431.

²⁰²*Proc. London Math. Soc.*, (2), 15, 1916, Records of meetings, Feb. 10, 1916, xxii.

²⁰³*Sphinx-Oedipe*, 1909, 1-26.

G. Wertheim, *Anfangsgründe der Zahlentheorie*, 1902.

G. Giraud, *Periodico di Mat.*, 21, 1906, 124-9.

F. Ferrari, *Suppl. al Periodico di Mat.*, 11, 1908, 36-8, 53, 75-6 (Cipolla).

P. Bachmann, *Niedere Zahlentheorie*, II, 1910, 97-101.

A. Aubry, *Assoc. franç. avanc. sc.*, 40, 1911, 53-4; 42, 1913; *l'enseignement math.*, 1911, 399; 1913, 215-6, 223.

*M. Kiseljak, *Beiträge zur Theorie der vollkommenen Zahlen*, *Progr. Agram*, 1911.

*J. Vaës, *Wiskundig Tijdschrift*, 8, 1911, 31, 173; 9, 1912, 120, 187.

J. Fitz-Patrick, *Exercices Math.*, ed. 3, 1914, 55-7.

MULTIPLY PERFECT NUMBERS.

A multiply perfect or pluperfect number n is one the sum of whose divisors, including n and 1, is a multiple of n . If the sum is mn , m is called the multiplicity of n . For brevity, a multiply perfect number of multiplicity m shall be designated by P_m . Thus an ordinary perfect number is a P_2 . Although Robert Recorde³⁹ in 1557 cited 120 as an abundant number, since the sum of its parts is 240, such numbers were first given names and investigated by French writers in the seventeenth century. As a P_3 equals one-half of the sum of its aliquot divisors or parts (divisors $< P_3$), it was called a sous-double; a P_4 equals one-third of the sum of its aliquot parts and was called a sous-triple; a P_5 a sous-quadruple; etc.

F. Marin Mersenne proposed to R. Descartes³⁰⁰ the problem to find a sous-double other than $P_3^{(1)} = 120 = 2^3 \cdot 3 \cdot 5$. The latter did not react on the question until seven years later.

Mersenne³⁰¹ mentioned (in the *Epistre*) the problem to find a P_4 , a P_5 or a P_m , a P_3 besides 120, and a rule to find as many as one pleases. He remarked (p. 211) that the P_3 120, the P_4 240 [for 30240?] and all other abundant numbers can signify the most fruitful natures.

Pierre de Fermat³⁰² referred in 1636 to his former [lost] letter in which he gave "the proposition concerning aliquot parts and the construction to find an infinitude of numbers of the same nature." He³⁰³ found the second P_3 , viz., $P_3^{(2)} = 672 = 2^5 \cdot 3 \cdot 7$.

Mersenne³⁰⁴ stated that Fermat found the P_3 672 and knew infallible rules and analysis to find an infinitude of such numbers. He³⁰⁵ later gave [Fermat's] method of finding such P_3 : Begin with the geometric

³⁰⁰Oeuvres de Descartes, 1, Paris, 1897, p. 229, line 28, letter from Descartes to Mersenne, Oct or Nov., 1631.

³⁰¹Les Preludes de l'Harmonie Universelle ou Questions Curieuses, Utiles aux Predicateurs, aux Theologiens, Astrologues, Medecins, & Philosophes, Paris, 1634.

³⁰²Oeuvres de Fermat, 2, Paris, 1894, p. 20, No. 3, letter to Mersenne, June 24, 1636.

³⁰³Oeuvres de Fermat, 2, p. 66 (French transl. 3, p. 288), 2, p. 72, letters to Mersenne and Roberval, Sept., 1636.

³⁰⁴Harmonie Universelle, Paris, 1636, *Premiere Preface Generale* (preceded by a preface of two pages), unnumbered page 9, remark 10. Extract in Oeuvres de Fermat, 2, 1894, 20-21.

³⁰⁵Mersenne, *Seconde Partie de l'Harmonie Universelle*, Paris, 1637. Final subdivision: *Nouvelles Observations Physiques et Mathématiques*, p. 26, Observation 13. Extract in Oeuvres de Fermat, 2, 1894, p. 21.

progression 2, 4, 8, . . . Subtract unity and place the remainders above the former. Add unity and place the sums below. Then if the quotient of the $(n+3)$ th number of the top line by the n th number of the bottom line is a prime, its triple multiplied by the $(n+2)$ th number of the middle line is a P_3 . Thus if $n=1$, $15/3$ is a prime and $3 \cdot 5 \cdot 8 = 120$ is a P_3 . For $n=3$, $63/9$ is a prime and $3 \cdot 7 \cdot 32 = 672$ is a P_3 . [This rule thus states in effect that $3 \cdot 2^{n+2}p$ is a P_3 if $p = (2^{n+3} - 1)/(2^n + 1)$ is a prime.]

The third P_3 , discovered by André Jumeau, Prior of Sainte-Croix, is

$$P_3^{(3)} = 523776 = 2^9 \cdot 3 \cdot 11 \cdot 31.$$

In April, 1638, he communicated it to Descartes³⁰⁶ and asked for the fourth P_3 (the fifth and last of St. Croix's challenge problems).

Descartes³⁰⁷ stated that the rule³⁰⁸ of Fermat furnishes no P_3 other than 120 and 672 and judged that Fermat did not find these numbers by the formula, but accommodated the formula to them, after finding them by trial.

Descartes³⁰⁸ answered the challenge of St. Croix with the fourth P_3 ,

$$P_3^{(4)} = 1476304896 = 2^{13} \cdot 3 \cdot 11 \cdot 43 \cdot 127.$$

Soon afterwards Descartes³⁰⁹ announced the following six P_4 :

$$\begin{aligned} P_4^{(1)} &= 30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7, \\ P_4^{(2)} &= 32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13, \\ P_4^{(3)} &= 23569920 = 2^9 \cdot 3^3 \cdot 5 \cdot 11 \cdot 31, \\ P_4^{(4)} &= 142990848 = 2^9 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31, \\ P_4^{(5)} &= 66433720320 = 2^{13} \cdot 3^3 \cdot 5 \cdot 11 \cdot 43 \cdot 127, \\ P_4^{(6)} &= 403031236608 = 2^{13} \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 127, \end{aligned}$$

and the sous-quadruple

$$P_5^{(1)} = 14182439040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19.$$

He stated that his analysis had led him to a method which would require time to explain in the form of a rule, but that he could find, for example, a sous-centuple, necessarily very large.

Fermat apparently responded to the fifth challenge problem of St. Croix on the fourth P_3 . Without warrant, Descartes³¹⁰ suspected that Fermat had not found independently the fourth P_3 , but had learned from some one in Paris of its earlier discovery by Descartes. Fermat³¹¹ indicated that he possessed an analytic method by which he could solve all questions con-

³⁰⁶Oeuvres de Descartes, 2, Paris, 1898, p. 428, p. 167 (latter without name of St. Croix); cf. Oeuvres de Fermat, 2, 1894, pp. 63-64.

³⁰⁷Oeuvres de Descartes, 2, 1898, p. 148, letter to Mersenne, May 27, 1638.

³⁰⁸Oeuvres de Descartes, 2, 1898, 167, letter to Mersenne, June 3, 1638.

³⁰⁹Oeuvres de Descartes, 2, 1898, 250-1, letter to Mersenne, July 13, 1638. In June, 1645, Descartes, 4, 1901, p. 229, again mentioned the first two of these P_4 .

³¹⁰Oeuvres de Descartes, 2, 1898, 273, letter to Mersenne, July 27, 1638.

³¹¹Oeuvres de Fermat, 2, 1894, p. 165, No. 4; p. 176, No. 1; letters to Mersenne, Aug. 10 and Dec. 26, 1638.

cerning aliquot parts, apart from the testing of the primality of a number n , knowing no method except the trial of each number $< \sqrt{n}$ as a divisor.

Descartes³¹² gave the following rules for multiply perfect numbers:

- I. If n is a P_3 not divisible by 3, then $3n$ is a P_4 .
- II. If a P_3 is divisible by 3, but by neither 5 nor 9, then $45P_3$ is a P_4 .
- III. If a P_3 is divisible by 3, but not by 7, 9 or 13, then $3 \cdot 7 \cdot 13 P_3$ is a P_4 .
- IV. If n is divisible by 2^9 , but by no one of the numbers 2^{10} , 31, 43, 127, then $31n$ and $16 \cdot 43 \cdot 127n$ are proportional to the sums of their aliquot parts.
- V. If n is not divisible by 3 and if $3n$ is a P_{4k} , then n is a P_{3k} .

By applying rule II to $P_3^{(2)}$, $P_3^{(3)}$, $P_3^{(4)}$, Descartes obtained his $P_4^{(1)}$, $P_4^{(3)}$, $P_4^{(5)}$. By applying rule III to $P_3^{(1)}$, $P_3^{(3)}$, $P_3^{(4)}$, he obtained his $P_4^{(2)}$, $P_4^{(4)}$, $P_4^{(6)}$.

In the same letter, Descartes expressed to Mersenne a desire to know what Frenicle de Bessy had found on this subject. Frenicle wrote direct to Descartes, who in his reply³¹³ expressed his astonishment that Frenicle should regard as sterile the above rules for finding P_4 , since Descartes had deduced by them six P_4 from four P_3 , at a time when Mersenne had stated to Descartes that it was thought to be impossible to find any at all. Descartes stated that, since one can find an infinity of such rules, one has the means of finding an infinitude of P_m . From one of Frenicle's P_5 (communicated to Descartes by Mersenne),

$$P_5^{(2)} = 30823866178560 = 2^{10} 3^5 5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 23 \cdot 89,$$

Descartes (p. 475) derived the smaller P_5 :

$$P_5^{(3)} = 31998395520 = 2^7 3^5 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 19.$$

Mersenne³¹⁴ listed various P_m due to his correspondents, without citation of names. He listed the above $P_3^{(i)}$ ($i=1, 2, 3, 4$) and remarked that "un excellent esprit"³¹⁵ found that when

$$P_3^{(5)} = 459818240 = 2^8 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73$$

is multiplied by 3, the product is a P_4 :

$$P_4^{(7)} = 2^8 3 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73,$$

attributed to Lucas³²¹ by Carmichael.³³⁴

³¹²Oeuvres, 2, 1898, 427-9, letter to Mersenne, Nov. 15, 1638.

³¹³Oeuvres de Descartes, 2, 1898, 471, letter to Frenicle, Jan. 9, 1639.

³¹⁴Les Nouvelles Pensees de Galilei, traduit d'Italien en François, Paris, 1639, Preface, pp. 6-7. Quoted in Oeuvres de Descartes, 10, Paris, 1908, pp. 564-6, and in Oeuvres de Fermat, 4, 1912, pp. 65-66.

³¹⁵Frenicle de Bessy, according to the editors of the Oeuvres de Fermat, 2, 1894, p. 255, note 2; 4, 1912, p. 65, note 2 (citing Oeuvres de Descartes, 2, letter Descartes to Mersenne, Nov. 15, 1638, pp. 419-448 [p. 429]). It is clear that the discoverers Fermat, St. Croix, and Descartes of the $P_i^{(i)}$ ($i=2, 3, 4$) are not meant. It is attributed to Legendre³¹⁹ by Carmichael.³³⁴

There are listed Descartes' six P_4 and $P_5^{(1)}$, Frenicle's $P_5^{(2)}$, and also

$$P_4^{(8)} = 45532800 = 2^7 3^3 5^2 17 \cdot 31,$$

$$P_4^{(9)} = 43861478400 = 2^{10} 3^3 5^2 23 \cdot 31 \cdot 89,$$

and the erroneous P_5 508666803200 (not divisible by $5^2 + 5 + 1$), probably a misprint for the correct P_5 (in the list by Lehmer³²³):

$$P_5^{(4)} = 518666803200 = 2^{11} 3^3 5^2 7^2 13 \cdot 19 \cdot 31.$$

A part of these P_m , but no new ones, were mentioned by Mersenne⁶⁰ in 1644; the least P_3 is stated to be 120. (*Oeuvres de Fermat*, 4, 66–7.)

In 1643 Fermat³¹⁶ cited a few of the P_m he had found:

$$P_3^{(6)} = 51001180160 = 2^{14} 5 \cdot 7 \cdot 19 \cdot 31 \cdot 151,$$

$$P_4^{(10)} = 3P_3^{(6)},$$

$$P_4^{(11)} = 14942123276641920 = 2^7 3^6 5 \cdot 17 \cdot 23 \cdot 137 \cdot 547 \cdot 1093,$$

$$P_5^{(5)} = 1802582780370364661760 = 2^{20} 3^3 5 \cdot 7^2 13^2 19 \cdot 31 \cdot 61 \cdot 127 \cdot 337,$$

$$P_5^{(6)} = 87934476737668055040 = 2^{17} 3^{55} 7^3 13 \cdot 19^2 37 \cdot 73 \cdot 127,$$

$$P_6^{(1)} = 2^{23} 3^7 5^3 7^4 11^3 13^3 17^2 31 \cdot 41 \cdot 61 \cdot 241 \cdot 307 \cdot 467 \cdot 2801,$$

$$P_6^{(2)} = 2^{27} 3^5 5^3 7 \cdot 11 \cdot 13^2 19 \cdot 29 \cdot 31 \cdot 43 \cdot 61 \cdot 113 \cdot 127.$$

He stated that he possessed a general method of finding all P_m .

Replying to Mersenne's query as to the ratio of

$$P_6^{(3)} = 2^{36} 3^{85} 5^{11} 13^2 19 \cdot 31^2 43 \cdot 61 \cdot 83 \cdot 223 \cdot 331 \cdot 379 \cdot 601 \cdot 757 \\ \times 1201 \cdot 7019 \cdot 823543 \cdot 616318177 \cdot 100895598169$$

to the sum of its aliquot parts, Fermat³¹⁷ stated that it is a P_6 , the prime factors of the final factor being 112303 and 898423 [on the finding of these factors, see Ch. XIV, references 23, 92, 94, 103]. Note that $823543 = 7^7$.

Descartes³¹⁸ constructed $P_3^{(2)} = 672 = 21 \cdot 32$ by starting with 21 and noting that $\sigma(21) = 32$, $\sigma(32) = 63 = 3 \cdot 21$, for σ defined as on p. 53.

Mersenne⁶¹ noted that if a P_3 is not divisible by 3, then $3P_3$ is a P_4 [rule I of Descartes³¹²]; if a P_5 is not divisible by 5, then $5P_5$ is a P_6 , etc. He stated that there had been found 34 P_4 , 18 P_5 , 10 P_6 , 7 P_7 , but no P_8 so far.

In 1652, J. Broschius (*Apologia*,⁵⁴ p. 162) cited the $P_4^{(1)}$ [of Descartes³⁰⁹]. The P_3 120 and 672 are mentioned in the 1770 edition of Ozanam's⁷⁹ *Récréations*, I, p. 35, and in Hutton's translation of Montucla's⁹⁹ edition, I, p. 39.

A. M. Legendre³¹⁹ determined the P_m of the form $2^a \alpha \beta \gamma \dots$, where $\alpha, \beta, \gamma, \dots$ are distinct odd primes, for $m = 3, n \leq 8$; $m = 4, n = 3, 5$; $m = 5, n = 7$. No new P_n were found.

³¹⁶*Oeuvres*, 2, 1894, p. 247 (261), letter to Carcavi; *Varia opera*, p. 178; *Précis des oeuvres math. de Fermat*, par E. Brassinne, Toulouse, 1853, p. 150.

³¹⁷*Oeuvres de Fermat*, 2, 1894, 255, letter to Mersenne, April 7, 1643. The editors (p. 256, note) explained the method of factoring probably used by Fermat. The sum of the aliquot parts of 2^{36} is $223N$, where $N = 616318177$, and the sum of the aliquot parts of N is $2 \cdot 7^7 M$, $M = 898423$. As M does not occur elsewhere in P_6 , it is to be expected as a factor of the final factor of P_6 .

³¹⁸Manuscript published by C. Henry, *Bull. Bibl. Storia Sc. Mat. e Fis.*, 12, 1879, 714.

³¹⁹*Thorie des nombres*, 3d ed., vol. 2, Paris, 1830, 146–7; German transl. by H. Maser, Leipzig, 2, 1893, 141–3. The work for $m = 3$ was reproduced by Lucas³²⁰ without reference.

E. Lucas³²⁰ gave a table of P_m of the form $2^{n-1}(2^n-1)N$ which includes only 15 of the 26 P_m given above and no additional P_m , $m>2$, except two erroneous P_5 :

$$2^{10}3^45 \cdot 7^2 \cdot 11^2 \cdot 19 \cdot 23 \cdot 89, \quad 2^{17}5 \cdot 7^2 13 \cdot 19^2 37 \cdot 73 \cdot 127,$$

attributed elsewhere³²¹ by him to Fermat. If we replace 7^2 by 7 in the former, we obtain a correct P_5 listed by Carmichael.³³²

$$P_5^{(7)} = 2^{10}3^45 \cdot 7 \cdot 11^2 19 \cdot 23 \cdot 89.$$

If in the second, we replace $5 \cdot 7^2$ by $3^5 \cdot 5 \cdot 7^3$ we obtain Fermat's $P_5^{(6)}$.

A. Desboves³²² noted that 120 and 672 are the only P_3 of the form $2^n \cdot 3 \cdot p$, where p is a prime.

D. N. Lehmer³²³ gave the additional P_m :

$$\begin{aligned} P_4^{(12)} &= 2^2 3^2 5 \cdot 7^2 13 \cdot 19, \\ P_4^{(13)} &= 2^8 3^2 7^2 13 \cdot 19^2 37 \cdot 73 \cdot 127, \\ P_5^{(8)} &= 2^{21} 3^6 5^2 7 \cdot 19 \cdot 23^2 31 \cdot 79 \cdot 89 \cdot 137 \cdot 547 \cdot 683 \cdot 1093, \\ P_6^{(4)} &= 2^{19} 3^6 5^3 7^2 11 \cdot 13 \cdot 19 \cdot 23 \cdot 31 \cdot 41 \cdot 137 \cdot 547 \cdot 1093, \\ P_6^{(5)} &= 2^{24} 3^8 5 \cdot 7^2 11 \cdot 13 \cdot 17 \cdot 19^2 31 \cdot 43 \cdot 53 \cdot 127 \cdot 379 \cdot 601 \cdot 757 \cdot 1801. \end{aligned}$$

He readily proved that a P_3 contains at least 3 distinct prime factors, a P_4 at least 4, a P_5 at least 6, a P_6 at least 9, a P_7 at least 14.

J. Westlund³²⁴ proved that $2^3 \cdot 3 \cdot 5$ and $2^5 \cdot 3 \cdot 7$ are the only P_3 of the form $p_1^a p_2^b p_3$, where the p 's are primes and $p_1 < p_2 < p_3$. He³²⁵ proved that the only $P_3 = p_1^a p_2 p_3 p_4$, $p_1 < p_2 < p_3 < p_4$, is $P_3^{(3)} = 2^9 \cdot 3 \cdot 11 \cdot 31$.

A. Cunningham³²⁶ considered P_m of the form $2^{q-1}(2^q-1)F$, where F is to be suitably determined. There exists at least one such P_m for every q up to 39, except 33, 35, 36, and one for $q=45, 51, 62$. Of the 85 P_m found, the only one published is the largest one, viz., for $q=62$, giving $P_6^{(6)}$ with

$$F = 3^7 5^4 7^2 11 \cdot 13 \cdot 19^2 23 \cdot 59 \cdot 71 \cdot 79 \cdot 127 \cdot 157 \cdot 379 \cdot 757 \cdot 43331 \cdot 3033169;$$

while none have $m>6$, and for $m=3$ at most one has a given q . He found in 1902 (but did not publish) the two $P_7 = 2^{46}(2^{47}-1)F$, where

$$\begin{aligned} F &= C \cdot 19^2 127 \text{ or } C \cdot 19^4 151 \cdot 911, \\ C &= 3^{15} \cdot 5^3 \cdot 7^5 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 89 \cdot 97 \cdot 193 \cdot 442151. \end{aligned}$$

R. D. Carmichael³²⁸ has shown that there exists no odd P_m with only three distinct prime factors; that $2^3 \cdot 3 \cdot 5$ and $2^5 \cdot 3 \cdot 7$ are the only P_m with only

³²⁰Bull. Bibl. e Storia Mat. e Fis., 10, 1877, 286. In $2^3 \cdot 3 \cdot 5 \cdot 7$, listed as a P_4 , 3 is a misprint for 3^2 .

³²¹Lucas, Théorie des Nombres, 1, Paris, 1891, 380. Here the factor $11^3 13^3$ of Fermat's $P_5^{(6)}$ is given erroneously as $11 \cdot 13^2$, while the $P_5^{(6)}$ of Descartes is attributed to Fermat.

³²²Questions d'Algèbre, 2d ed., 1878, p. 490, Ex. 24.

³²³Annals of Math., (2), 2, 1900-1, 103-4.

³²⁴Annals of Math., (2), 2, 1900-1, 172-4.

³²⁵Annals of Math., (2), 3, 1901-2, 161-3.

³²⁶British Association Reports, 1902, 528-9.

³²⁸American Math. Monthly, 13, Feb., 1906, 35-36.

three distinct prime factors;³²⁹ that those with only four distinct prime factors are³³⁰ the $P_3^{(3)}$ of St. Croix³⁰⁶ and the $P_4^{(1)}$ of Descartes,³⁰⁹ and that the even P_m with five³³¹ distinct prime factors are $P_3^{(4)}$, $P_4^{(2)}$, $P_4^{(3)}$ of Descartes^{308, 309} and $P_4^{(8)}$ of Mersenne.³¹⁴

Carmichael^{331a} stated and J. Westlund proved that if $n > 4$, no P_n has only n distinct prime factors.

Carmichael's³³² table of multiply perfect numbers contains the misprint 1 for the final digit 0 of Descartes' $P_4^{(3)}$, and the erroneous entry 919636480 in place of its half, viz., $P_3^{(5)}$ of Mersenne.³¹⁴ The only new P_m is

$$P_6^{(7)} = 2^{15} 3^{55} 7^2 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 43 \cdot 257.$$

All $P_m < 10^9$ were determined; only known ones were found.

Carmichael³³³ gave an erroneous P_5 and the new P_4 :

$$P_4^{(14)} = 2^{14} 3^{27} 13 \cdot 19 \cdot 231 \cdot 127 \cdot 151,$$

$$P_4^{(15)} = 2^{25} 3^5 5^2 19 \cdot 31 \cdot 683 \cdot 2731 \cdot 8191,$$

$$P_4^{(16)} = 2^{25} 3^6 5 \cdot 19 \cdot 23 \cdot 137 \cdot 547 \cdot 683 \cdot 1093 \cdot 2731 \cdot 8191.$$

Carmichael and T. E. Mason³³⁴ gave a table which includes the above listed 10 P_2 , 6 P_3 , 16 P_4 , 8 P_5 , 7 P_6 , together with 204 new multiply perfect numbers P_i ($i=3, \dots, 7$). Of the latter, 29 are of multiplicity 7, each having a very large number of prime factors. No P_7 had been previously published.

[As a generalization, consider numbers n the sum of the k th powers of whose divisors $< n$ is a multiple of n . For example, $n=2p$, where p is a prime $8h \pm 3$ and k is such that $2^k + 1$ is divisible by p ; cases are $p=3$, $k=1$; $p=5$, $k=2$; $p=11$, $k=5$; $p=13$, $k=6$.]

AMICABLE NUMBERS.

Two numbers are called amicable* if each equals the sum of the aliquot divisors of the other.

According to Iamblichus⁴ (pp. 47-48), "certain men steeped in mistaken opinion thought that the perfect number was called love by the Pythagoreans on account of the union of different elements and affinity which exists in it; for they call certain other numbers, on the contrary, amicable numbers, adopting virtues and social qualities to numbers, as 284 and 220, for the parts of each have the power to generate the other, according to the rule of friendship, as Pythagoras affirmed. When asked what is a friend, he replied, 'another I,' which is shown in these numbers. Aristotle so defined a friend in his Ethics."

³²⁹Annals of Math., (2), 7, 1905-6, 153; 8, 1906-7, 49-56; 9, 1907-8, 180, for a simpler proof that there is no $P_3 = p_1^a p_2^b p_3^c$, $c > 1$.

³³⁰Annals of Math., (2), 8, 1906-7, 149-158.

³³¹Bull. Amer. Math. Soc., 15, 1908-9, pp. 7-8. Fr. transl., Sphinx-Oedipe, Nancy, 5, 1910, 164-5.

^{331a}Amer. Math. Monthly, 13, 1906, 165.

³³²Bull. Amer. Math. Soc., 13, 1906-7, 383-6. Fr. transl., Sphinx-Oedipe, Nancy, 5, 1910, 161-4.

³³³Sphinx-Oedipe, Nancy, 5, 1910, 166.

³³⁴Proc. Indiana Acad. Sc., 1911, 257-270.

*Amiable, agreeable, befreundete, verwandte.

In the ninth century the Arab Thâbit ben Korrah¹⁰ (prop. 10) noted that 2^nh and $2^n s$ are amicable numbers if

$$(1) \quad h = 3 \cdot 2^n - 1, \quad t = 3 \cdot 2^{n-1} - 1, \quad s = 9 \cdot 2^{2n-1} - 1$$

are primes > 2 , literally, if

$$h = z + 2^n, \quad t = z - 2^{n-1}, \quad z = 1 + 2 + \dots + 2^n, \quad s = (2^{n+1} + 2^{n-2})2^{n+1} - 1.$$

The term used for amicable numbers was *se invicem amantes*. In the article in which F. Woepcke¹⁰ translated this Arabic manuscript into French, he noted that a definition of these numbers, called *congeneres*, occurs in the 51st treatise (on arithmetic) of Ikhovân Alḡafâ, manuscript 1105, anciens fonds arabes, p. 15, of the National Library of Paris.

Among Jacob's presents to Esau were 200 she-goats and 20 he-goats, 200 ewes and 20 rams (Genesis, XXXII, 14). Abraham Azulai³⁴⁹ (1570–1643), in commenting on this passage from the Bible, remarked that he had found written in the name of Rau Nachshon (ninth century A. D.): Our ancestor Jacob prepared his present in a wise way. This number 220 (of goats) is a hidden secret, being one of a pair of numbers such that the parts of it are equal to the other one 284, and conversely. And Jacob had this in mind; this has been tried by the ancients in securing the love of kings and dignatories.

Ibn Khaldoun³⁵⁰ related "that persons who have concerned themselves with talismans affirm that the amicable numbers 220 and 284 have an influence to establish a union or close friendship between two individuals. To this end a theme is prepared for each individual, one during the ascendancy of Venus, when that planet is in its exaltation and presents to the moon an aspect of love or benevolence; for the second theme the ascendancy should be in the seventh. On each of these themes is written one of the specified numbers, the greater (or that with the greater sum of its aliquot parts?) being attributed to the person whose friendship is sought."

The Arab El Madschrîṭi,³⁵¹ or el-Mağrîṭi, (†1007) of Madrid related that he had himself put to the test the erotic effect of "giving any one the smaller number 220 to eat, and himself eating the larger number 284."

Ibn el-Hasan^{351a} (†1320) wrote several works, including the "Memory of Friends," on the explanation of amicable numbers.

Ben Kalonymos^{351b} discussed amicable numbers in 1320 in a work written for Robert of Anjou, a fragment of which is in Munich (Hebr. MS. 290, f. 60). A knowledge of amicable numbers was considered necessary by Jochanan Allemanno (fifteenth century) to determine whether an aspect of the planets was friendly or not.

³⁴⁹Baale Brith Abraham [Commentary on the Bible], Wilna, 1873, 22. Quotation supplied by Mr. Ginsburg.

³⁵⁰Prolégomènes hist. d'Ibn Khaldoun, French transl. by De Slane, Notices et Extraits des Manuscrits de la Bibl. Impériale, Paris, 21, I, 1868, 178–9.

³⁵¹Manuscript Mağrîṭi; Steinschneider, Zur pseudoepigraphischen Literatur insbesondere der geheimen Wissenschaften des Mittelalters, Berlin, 1862, p. 37 (cf. p. 41).

^{351a}H. Suter, Abh. Gesch. Math. Wiss., 10, 1900, 159, § 389.

^{351b}Hebr. Bibl., VII, 91. Steinschneider, Zeitschrift der Morgenländischen Ges., 24, 1870, 369.

Alkalacadi,³⁵² a Spanish Arab (†1486), showed the method of finding the least amicable numbers 220, 284.

Nicolas Chuquet¹⁵ in 1484 and de la Roche²⁸ in 1538 cited the amicable numbers 220, 284, "de merueilleuse familiarite lung avec laultre." In 1553, Michael Stifel³² (folios 26v-27v) mentioned only this pair of amicable numbers. The same is true of Cardan,²⁷ of Peter Bungus⁴² (*Mysticae numerorum signif.*, 1585, 105), and of Tartaglia.³⁵³ Reference may be made also to Schwenter.⁵²

In 1634 Mersenne³⁰¹ (p. 212) remarked that "220 and 284 can signify the perfect friendship of two persons since the sum of the aliquot parts of 220 is 284 and conversely, as if these two numbers were only the same thing."

According to Mersenne's³⁰⁴ statement in 1636, Fermat³⁵⁴ found the second pair of amicable numbers

$$17296 = 2^4 \cdot 23 \cdot 47, \quad 18416 = 2^4 \cdot 1151,$$

and communicated to Mersenne³⁰⁵ the general rule: Begin with the geometric progression 2, 4, 8, . . . , write the prod-

ucts by 3 in the line below; subtract 1 from	5	11	23	47
the products and enter in the top row. The	2	4	8	16
bottom row is 6·12-1, 12·24-1, . . . When a	6	12	24	48
number of the last row is a prime (as 71) and		71	287	1151

the one (11) above it in the top row is a prime,
and the one (5) preceding that is also a prime, then $71 \cdot 4 = 284$, $5 \cdot 11 \cdot 4 = 220$
are amicable. Similarly for

$$1151 \cdot 16 = 18416, \quad 23 \cdot 47 \cdot 16 = 17296,$$

and so to infinity. [The rule leads to the pair $2^nh t$, 2^ns , where h , t , s are given by (1).]

Descartes³⁵⁵ gave the rule: Take (2 or) any power of 2 such that its triple less 1, its sextuple less 1, and the 18-fold of its square less 1 are all primes;* the product of the last prime by the double of the assumed power of 2 is one of a pair of amicable numbers. Starting with the powers 2, 8, 64, we get 284, 18416, 9437056, whose aliquot parts make 220, etc. Thus the third pair is

$$9363584 = 2^7 \cdot 191 \cdot 383, \quad 9437056 = 2^7 \cdot 73727.$$

Descartes³⁵⁶ stated that Fermat's rule agrees exactly with his own.

Although we saw that Mersenne quoted in 1637 the rule in Fermat's form and expressly attributed it to Fermat, curiously enough Mersenne³¹⁴ gave in 1639 the rule in Descartes' form, attributing it to "un excellent Géomètre" (meaning without doubt Descartes, according to C. Henry³⁵⁷),

³⁵²Manuscript in Bibliothèque Nationale Paris, a commentary on the arithmetic Talkhys of Ibn Albanna (13th cent.). Cf. E. Lucas, *L'arithmétique amusante*, Paris, 1895, p. 64.

³⁵³Quesiti et Inventiones, 1554, fol. 98 v.

³⁵⁴Oeuvres de Fermat, 2, 1894, p. 72, letter to Roberval, Sept. 22, 1636; p. 208, letter to Frenicle, Oct. 18, 1640.

³⁵⁵Oeuvres de Descartes, 2, 1898, 93-94, letter to Mersenne, Mar. 31, 1638.

*Evidently the numbers (1) if the initial power of 2 be 2^{n-1} .

³⁵⁶Oeuvres de Descartes, 2, 1898, 148, letter to Mersenne, May 27, 1638.

³⁵⁷Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 523.

and derived as did Descartes the first three pairs of amicable numbers from 2, 8, 64. We shall see that various later writers attributed the rule to Descartes.

Mersenne⁶⁰ again in 1644 gave the above three pairs of amicable numbers, the misprints in both³⁵⁸ of the numbers of the third pair being noticed at the end of his book, and stated there are others innumerable.

Mersenne⁶¹ in 1647 gave without citation of his source the rule in the form $2 \cdot 2^n s$, $2 \cdot 2^h t$, where $t = 3 \cdot 2^n - 1$, $h = 2t + 1$, $s = ht + h + t$ are primes [as in (1)].

Frans van Schooten,³⁵⁹ the younger, showed how to find amicable numbers by indeterminate analysis. Consider the pair $4x$, $4yz$ [x , y , z odd primes]; then

$$7 + 3x = 4yz, \quad 7 + 7y + 7z + 3yz = 4x.$$

Eliminating x , we get $z = 3 + 16/(y - 3)$. The case $y = 5$ gives $z = 11$, $x = 71$, yielding 284, 220. He proved that there are none of the type $2x$, $2yz$, or $8x$, $8yz$, and argued that no pair is smaller than 284, 220. For $16x$, $16yz$, he found $z = 15 + 256/(y - 15)$, which for $y = 47$ yields the second known pair. There are none of the type $32x$, $32yz$, or type $64x$, $64yz$. For $128x$, $128yz$, he got $z = 127 + 16384/(y - 127)$, which for $y = 191$ yields the third known pair. Finally, he quoted the rule of Descartes.

W. Leybourn⁶² stated in 1667 that "there is a fine harmony between these two numbers 220 and 284, that the aliquot parts of the one do make up the other . . . and this harmony is not to be found in many other numbers."

In 1696, Ozanam⁷³ gave in great detail the derivation of the three known pairs of "amiable" numbers by the rule as stated by Descartes, whose name was not cited. Nothing was added in the later editions.^{79, 99}

Paul Halcke³⁶⁰ gave Stifel's³² rule, as expressed by Descartes.³⁵⁵

E. Stone³⁶¹ quoted Descartes' rule in the incorrect form that $2^{2n}pq$ and $3 \cdot 2^n p$ are amicable if $p = 3 \cdot 2^n - 1$ and $q = 6 \cdot 2^n - 1$ are primes.

Leonard Euler³⁶² remarked that Descartes and van Schooten found only three pairs of amicable numbers, and gave, without details, a list of 30 pairs, all included in the later paper by Euler.³⁶⁴

G. W. Kraft³⁶³ considered amicable numbers of the type APQ , AR , where P , Q , R are primes not dividing A . Let a be the sum of all the divisors of A . Then

$$R + 1 = (P + 1)(Q + 1), \quad (R + 1)a = APQ + AR.$$

Assuming prime values of P and Q such that the resulting R is prime, he sought a number A for which A/a has the derived value. For $P = 3$, $Q = 11$,

³⁵⁸Not noticed in the correction (left in doubt) in *Oeuvres de Fermat*, 4, 1912, p. 250 (on pp. 66-7). One error is noted in Broschius⁶⁴, *Apologia*, 1652, p. 154.

³⁵⁹*Exercitationum mathematicarum libri quinque*, Ludg. Batav., 1657, liber V: sectiones triginta miscellaneas, sect. 9, 419-425. Quoted by J. Landen.⁸⁸

³⁶⁰*Deliciae Mathematicae, oder Math. Sinnen-Confect*, Hamburg, 1719, 197-9.

³⁶¹*New Mathematical Dictionary*, 1743 (under amicable).

³⁶²*De numeris amicabilibus*, *Nova Acta Eruditorum*, Lipsiae, 1747, 267-9; *Comm. Arith. Coll.*, II, 1849, 637-8.

³⁶³*Novi Comm. Ac. Petrop.*, 2, 1751, ad annum 1749, *Mem.*, 100-18.

then $A:a=3:5$; he took $A=3B$, 3^2B , 3^3B , but found no solution. For $P=5$, $Q=41$, we have $R=251$, $38A=21a$; set $A=49B$, whence $3\cdot 57b=38\cdot 7B$, where b is the sum of the divisors of B ; set $B=9C$, whence $C:c=13:14$, $C=13$, yielding the amicable numbers $5\cdot 41A$, $251A$, where $A=3^2\cdot 7^2\cdot 13=5733$ [the pair VII in Euler's³⁶² list and (7) in the table below]. Again, to make $A/a=3/8$, set $A=3B$, whence $a=4b$ and the condition is $b=2B$, whence B is a perfect number prime to 3. Using $B=28$, we get $A=84$. For use in such questions, Kraft gave a table of the sum of the divisors of each number ≤ 150 . He quoted the rule of Descartes.

L. Euler³⁶⁴ obtained, in addition to two special pairs, 62 pairs [including two false pairs] of amicable numbers of the type am , an , in which the common factor a is relatively prime to both m and n . He wrote $\int m$ for the sum of all the divisors of m . The conditions are therefore

$$\int m = \int n, \quad \int a \cdot \int m = a(m+n).$$

If m and n are both primes, then $m=n$ and we have a repeated perfect number. Euler treated five problems.

(1) Euler's problem 1 is to find amicable numbers apq , ar , where p , q , r , are distinct primes not dividing the given number a . From the first condition we have $r=xy-1$, where $x=p+1$, $y=q+1$. From the second,

$$xy \int a = a(2xy - x - y).$$

Let $a/(2a - \int a)$ equal b/c , a fraction in its lowest terms. Then

$$y = bx/(cx - b), \quad (cx - b)(cy - b) = b^2.$$

Thus x and y are to be found by expressing b^2 as a product of two factors, increasing each by b , and dividing the results by c .

(1₁) First, take $a=2^n$. Then $b=2^n$, $c=1$, $x, y=2^{n\pm k}+2^n$. Let $n-k=m$. Then

$$p=2^m(2^{2k}+2^k)-1, \quad q=2^m(1+2^k)-1, \quad r=2^{2m}(2^{2k+1}+2^{3k}+2^k)-1.$$

When these three are primes, $2^{m+k}pq$ and $2^{m+k}r$ are amicable. Euler noted that the rule communicated by Descartes to van Schooten is obtained by taking $k=1$, and stated that 1, 3, 6 are the only values ≤ 8 of m which yield amicable numbers (above³⁵⁵). For $k=2$ or 4, Euler remarked that r is divisible by 3; for $k=3$, $m<6$, and for $k=5$, $m\leq 2$, p , q , or r is composite.

(1₂) Take $a=2^nf$, where $f=2^{n+1}+e$ is a prime. Then $2a - \int a = e+1$. If $e+1$ divides a , we have $c=1$. Set $e+1=2^k$, $k\leq m$, $n=m+k$. Then

$$f=2^k(2^{m+1}+1)-1, \quad a=2^{m+k}f, \quad b=2^mf, \quad b^2=(x-b)(y-b).$$

For $k=1$, $f=2^{m+2}+1$ is to be a prime, whence $m+2$ is a power of 2. If $m=0$, $b=f=5$, and either $x=y$, $p=q$; or $x, y=6, 30$; $p, q=5, 29$, whereas p and q are to be distinct and prime to 10. If $m=2$, $f=17$, 68^2 is to be resolved into distinct even factors; in the four resulting cases, p, q, r are

³⁶⁴De numeris amicabilebus, Opuscula varii argumenti, 2, 1750, 23-107, Berlin; Comm. Arith., 1, 1849, 102-145. French transl. in Sphinx-Oedipe, Nancy, 1, 1906-7, Supplément I-LXXXVI.

not all prime. In the next case $m=6$, $f=257$, Euler examined only the case* $x-b=2^5 \cdot 257$, finding q composite.

For $k=2$, Euler excluded $m=1, 3$ [$m=4$ is easily excluded].

(1₃) For $k \geq n$ in (1₂), $c=2^m$, where $m=k-n$. Then

$$b=2^{n+1}+2^{m+n}-1=f$$

must be a prime. Thus we must take as the factors of b^2

$$2^m x - b = 1, \quad 2^m y - b = b^2,$$

whence $x=2^n+2^{n+1-m}$, $y=bx$. If $m=1$, one of

$$f=2^{n+2}-1, \quad p=2^{n+1}-1$$

has the factor 3 and yet must be a prime; hence $n=1$, $q=27$. If $m=2$, Euler treated the cases $n \leq 5$ and found (for $n=2$) the pair (4) of the table. [For $6 \leq n \leq 17$, f or p is composite.] For m odd and >1 , f or p has the factor 3. For $m=4$, $n \leq 17$, no solution results.

(1₄) For $a=2^n(g-1)(h-1)$, where the last two factors are prime, set $d=2a-f$. Then

$$(g-2^{n+1})(h-2^{n+1})=d-2^{n+1}+2^{2n+2}.$$

Euler treated the cases $n \leq 3$, $d=4, 8, 16$, finding only the pair (9).

(1₅) Special odd values of a led (§§56-65) to seven pairs (5)-(8), (11)-(13). The cases $a=3^3 \cdot 5$, $3^2 \cdot 7^2 \cdot 13 \cdot 19$ were unfruitful.

(2) Euler's problem 2 is to find amicable numbers apq , ars , where p, q, r, s are distinct primes not dividing the given number a . Since $\int p \cdot \int q = \int r \cdot \int s$, we may set

$$p=\alpha x-1, \quad q=\beta y-1, \quad r=\beta x-1, \quad s=\alpha y-1.$$

We set $\int a : a = 2b - c : b$, where b and c are relatively prime. The second condition $\int a \cdot \int pq = a(pq+rs)$ gives

$$ca\beta xy = b(a+\beta)(x+y) - 2b.$$

Multiply it by $ca\beta$. Then

$$[ca\beta x - b(a+\beta)][ca\beta y - b(a+\beta)] = b^2(a+\beta)^2 - 2bca\beta.$$

Given α, β, a and hence b, c , we are to express the second member as a product of two factors and then find x, y .

For $\alpha=1, \beta=3, a=2^n$, Euler obtained the pairs (α), (28). For $\alpha=2, \beta=3, a=3^2 \cdot 5 \cdot 13$, he got (32); for $\alpha=1, \beta=4, a=3^3 \cdot 5$, (30). The ratio $\alpha:\beta$ may be more complex, as 5:21 or 1:102, in (γ). As noted by K. Hunrath,^{364a} the numbers (γ) are not amicable. Nor are the ratios as given, although these ratios result if we replace 8563 by $8567=13 \cdot 659$. This false pair occurs as XIII in Euler's³⁶² list.

(3) Problem 3 is derived from problem 2 by replacing s by a number f not necessarily prime. Let h be the greatest common divisor of $\int f = hg$ and $p+1 = hx$. Then $r+1 = xy, q+1 = gy$. Also

$$ghxy \int a \equiv \int (afr) = a(pq+fr) \equiv a \{ (hx-1)(gy-1) + f(xy-1) \}.$$

*All the remaining cases are readily excluded.

^{364a}Bibliotheca Math., (3), 10, 1909-10, 80-81.

Multiply by b/a and replace $b\int a$ by $2ab - ac$ [see case (1)]. Thus

$$exy - b\hbar x - bgy = b(f-1), \quad e \equiv bf - bgh + cgh.$$

Thus $L \equiv b^2gh + be(f-1)$ is to be expressed as the product PQ of two factors and they are to be equated to $ex - bg$, $ey - bh$. The case $a=2$ is unfruitful.

(3₁) Let $a=4$. Then $b=4$, $c=1$, $e=4f-3gh$. The case $f=3$ is excluded since it gives $e=0$. For $f=5$, $g=2$, $h=3$, we again get (a) and also (β). For $f=5$, $g=1$, $h=6$, we get only the same two pairs. For a prime $f \geq 7$, no new solutions are found. For $f=5 \cdot 13$, (51) results.

(3₂) Let $a=8$, whence $b=8$, $c=1$. The cases $f=11$, 13 are fruitless, while $f=17$ yields (16). The least composite f yielding solutions is $11 \cdot 23$, giving (44), (45), (46). This fruitful case led Euler to the more convenient notations (§88) $M=hP$, $N=gQ$, $L=PQ$. The problem is now to resolve $L \int f$ into two factors, M , N , such that

$$p = \frac{M+b\int f}{e} - 1, \quad q = \frac{N+b\int f}{e} - 1$$

are integers and primes, while in $r+1 = (p+1)(q+1)/\int f$, r is a prime.

(3₃) Let $a=16$. For $f=17$, we obtain the pairs (21), (22); for $f=19$, (23); for $f=23$, (17), (19), (20); for $f=47$, (18); for $f=17 \cdot 167$, (49). Cases $f=31$, $17 \cdot 151$ are fruitless [the last since 129503 has the factor 11, not noticed by Euler].

(3₄) For $a=3^3 \cdot 5$ or $3^2 \cdot 7 \cdot 13$, $b=9$, $c=2$; the first a with $f=7$ yields (30).

(4) Problem 4 relates to amicable numbers $agpq$, ahr , where p , q , r are primes. Eventually he took also g and h as primes. We may then set $g+1=km$, $h+1=kn$. For $m=1$, $n=3$, $a=4$ or 8 , no amicables are found. For $m=3$, $n=1$, the cases $a=10$, $k=8$ and $a=3^3 \cdot 5$, $k=8$, yield (38), (55).

(5) Euler's final problem 5 is of a new type. He discussed amicable numbers zap , zbq , where a and b are given numbers, p and q are unknown primes, while z is unknown but relatively prime to a , b , p , q . Set $\int a : \int b = m : n$, where m and n are relatively prime. Since $(p+1)\int a = (q+1)\int b$, we may set $p+1=nx$, $q+1=mx$. The usual second condition gives

$$nx \int a \cdot \int z = za(nx-1) + zb(mx-1), \quad \frac{z}{\int z} = \frac{nx \int a}{(na+mb)x - a - b}.$$

Let the latter fraction in its lowest terms be r/s . Then $z=kr$, $\int z=ks$. Since $\int(kr) \geq k \int r$, we have $s \geq \int r$. Hence we have the useful theorem: if $z : \int z = r' : s'$, $s' < \int r'$, then r' and s' have a common factor > 1 .

(5₁) The unfruitful case $a=3$, $b=1$, was treated like the next.

(5₂) Let $a=5$, $b=1$, whence $m=6$, $n=1$, $z : \int z = 6x : 11x - 6$. By the theorem in (5), x must be divisible by 2 or 3. Euler treated the cases $x=3(3t+1)$, $x=2(2t+1)$. But this classification is both incomplete and

overlapping. Since $p = x - 1$ is to be prime, x is even (since $x = 3$ makes z divisible by $p = 2$). Hence $x = 2P, z = 6P : 11P - 3$. By the theorem in (5), $6P$ and $11P - 3$ have a common factor 2 or 3, so that P is either odd or divisible by 6. For $P = 6l$, the ratio is that of $12b$ to $22l - 1$, which as before must have the common factor 3, whence $l = 3t + 1$. Then $z : \int z = 4(3t + 1) : 22t + 7$, a ratio of relatively prime numbers, whence $22t + 7 \geq \int 4(3t + 1)$, and hence $t = 2k, k = 0$ or $k > 3$. For $k = 0$, we obtain the pair 220, 284. The next value > 3 of k for which $p = x - 1$ and $q = 6x - 1$ are primes is $k = 6$, giving $p = 443, q = 2663$, numbers much larger than those in the (unnecessary) cases treated by Euler. Then $z : \int z = 4 \cdot 37 : 271$; set $z = 37^e d$, d not divisible by 37; the cases $e = 1, 2, 3$ are excluded by the theorem in (5). For the remaining case P odd, $P = 2Q + 1$, Euler treated those values ≤ 100 of Q , and also $Q = 244$, for which p and q are primes and obtained the pair in (1₃), two pairs in (1₅), and (14), (15).

(5₃) Euler treated in §§112-7 various sets a, b , and obtained (a) and nine new pairs given in the table.

In the following table of the 64 pairs of amicable numbers obtained by Euler, the numbering of any pair is the same as in Euler's list, but the pairs have been rearranged so that it becomes easy to decide if any proposed pair is one of Euler's. As noted by F. Rudio,^{364b} (37) contained the misprint 3^3 for 3^2 , while (γ) and (34) are erroneous, 220499 being composite (311·709); he checked that all other entries are correct.

(39) $2 \cdot 5 \left\{ \begin{smallmatrix} 7 \cdot 19 \cdot 107 \\ 47 \cdot 359 \end{smallmatrix} \right.$	(38) $2 \cdot 5 \left\{ \begin{smallmatrix} 7 \cdot 60659 \\ 23 \cdot 29 \cdot 673 \end{smallmatrix} \right.$	(1) $2^2 \left\{ \begin{smallmatrix} 5 \cdot 11 \\ 71 \end{smallmatrix} \right.$	(51) $2^2 \left\{ \begin{smallmatrix} 5 \cdot 13 \cdot 1187 \\ 43 \cdot 2267 \end{smallmatrix} \right.$
(4) $2^2 \cdot 23 \left\{ \begin{smallmatrix} 5 \cdot 137 \\ 827 \end{smallmatrix} \right.$	(a) $2^2 \left\{ \begin{smallmatrix} 5 \cdot 131 \\ 17 \cdot 43 \end{smallmatrix} \right.$	(β) $2^2 \left\{ \begin{smallmatrix} 5 \cdot 251 \\ 13 \cdot 107 \end{smallmatrix} \right.$	(29) $2^2 \cdot 11 \left\{ \begin{smallmatrix} 17 \cdot 263 \\ 43 \cdot 107 \end{smallmatrix} \right.$
(9) $2^2 \cdot 13 \cdot 17 \left\{ \begin{smallmatrix} 389 \cdot 509 \\ 198899 \end{smallmatrix} \right.$	(46) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 23 \cdot 1619 \\ 647 \cdot 719 \end{smallmatrix} \right.$	(45) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 23 \cdot 1871 \\ 467 \cdot 1151 \end{smallmatrix} \right.$	(44) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 23 \cdot 2543 \\ 383 \cdot 1907 \end{smallmatrix} \right.$
(47) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 29 \cdot 239 \\ 191 \cdot 449 \end{smallmatrix} \right.$	(43) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 59 \cdot 173 \\ 47 \cdot 2609 \end{smallmatrix} \right.$	(40) $2^3 \left\{ \begin{smallmatrix} 11 \cdot 163 \cdot 191 \\ 31 \cdot 11807 \end{smallmatrix} \right.$	(16) $2^3 \left\{ \begin{smallmatrix} 17 \cdot 79 \\ 23 \cdot 59 \end{smallmatrix} \right.$
(48) $2^3 \left\{ \begin{smallmatrix} 17 \cdot 4799 \\ 29 \cdot 47 \cdot 59 \end{smallmatrix} \right.$	(60) $\left\{ \begin{smallmatrix} 2^3 \cdot 19 \cdot 41 \\ 2^5 \cdot 199 \end{smallmatrix} \right.$	(61) $\left\{ \begin{smallmatrix} 2^3 \cdot 41 \cdot 467 \\ 2^5 \cdot 19 \cdot 233 \end{smallmatrix} \right.$	(49) $2^4 \left\{ \begin{smallmatrix} 17 \cdot 167 \cdot 13679 \\ 809 \cdot 51071 \end{smallmatrix} \right.$
(21) $2^4 \left\{ \begin{smallmatrix} 17 \cdot 5119 \\ 239 \cdot 383 \end{smallmatrix} \right.$	(22) $2^4 \left\{ \begin{smallmatrix} 17 \cdot 10303 \\ 167 \cdot 1103 \end{smallmatrix} \right.$	(23) $2^4 \left\{ \begin{smallmatrix} 19 \cdot 1439 \\ 149 \cdot 191 \end{smallmatrix} \right.$	
(γ) $2^4 \left\{ \begin{smallmatrix} 19 \cdot 8563 \\ 83 \cdot 2039 \end{smallmatrix} \right.$ (false)	(2) $2^4 \left\{ \begin{smallmatrix} 23 \cdot 47 \\ 1151 \end{smallmatrix} \right.$	(50) $2^4 \left\{ \begin{smallmatrix} 23 \cdot 47 \cdot 9767 \\ 1583 \cdot 7103 \end{smallmatrix} \right.$	
(20) $2^4 \left\{ \begin{smallmatrix} 23 \cdot 467 \\ 103 \cdot 107 \end{smallmatrix} \right.$	(19) $2^4 \left\{ \begin{smallmatrix} 23 \cdot 479 \\ 89 \cdot 127 \end{smallmatrix} \right.$	(17) $2^4 \left\{ \begin{smallmatrix} 23 \cdot 1367 \\ 53 \cdot 607 \end{smallmatrix} \right.$	(36) $2^4 \cdot 67 \left\{ \begin{smallmatrix} 37 \cdot 2411 \\ 227 \cdot 401 \end{smallmatrix} \right.$
(18) $2^4 \left\{ \begin{smallmatrix} 47 \cdot 89 \\ 53 \cdot 79 \end{smallmatrix} \right.$	(25) $2^5 \left\{ \begin{smallmatrix} 37 \cdot 12671 \\ 227 \cdot 2111 \end{smallmatrix} \right.$	(26) $2^5 \left\{ \begin{smallmatrix} 53 \cdot 10559 \\ 79 \cdot 7127 \end{smallmatrix} \right.$	(24) $2^5 \left\{ \begin{smallmatrix} 59 \cdot 1103 \\ 79 \cdot 827 \end{smallmatrix} \right.$
(27) $2^5 \left\{ \begin{smallmatrix} 79 \cdot 11087 \\ 383 \cdot 2309 \end{smallmatrix} \right.$	(3) $2^7 \left\{ \begin{smallmatrix} 191 \cdot 383 \\ 73727 \end{smallmatrix} \right.$	(28) $2^8 \left\{ \begin{smallmatrix} 383 \cdot 9203 \\ 1151 \cdot 3067 \end{smallmatrix} \right.$	
(37) $3^2 \cdot 5 \left\{ \begin{smallmatrix} 7 \cdot 11 \cdot 29 \\ 31 \cdot 89 \end{smallmatrix} \right.$	(5) $3^2 \cdot 7 \cdot 13 \left\{ \begin{smallmatrix} 5 \cdot 17 \\ 107 \end{smallmatrix} \right.$	(7) $3^2 \cdot 7^2 \cdot 13 \left\{ \begin{smallmatrix} 5 \cdot 41 \\ 251 \end{smallmatrix} \right.$	(52) $3^2 \cdot 7 \cdot 13 \left\{ \begin{smallmatrix} 5 \cdot 17 \cdot 1187 \\ 131 \cdot 971 \end{smallmatrix} \right.$
(15) $3^2 \cdot 7 \cdot 13 \cdot 41 \cdot 163 \left\{ \begin{smallmatrix} 5 \cdot 977 \\ 5867 \end{smallmatrix} \right.$	(14) $3^2 \cdot 7^2 \cdot 13 \cdot 97 \left\{ \begin{smallmatrix} 5 \cdot 193 \\ 1163 \end{smallmatrix} \right.$	(10) $3^2 \cdot 5 \cdot 19 \cdot 37 \left\{ \begin{smallmatrix} 7 \cdot 887 \\ 7103 \end{smallmatrix} \right.$	
(35) $3^2 \cdot 5 \cdot 19 \left\{ \begin{smallmatrix} 7 \cdot 227 \\ 37 \cdot 47 \end{smallmatrix} \right.$	(8) $3^2 \cdot 5 \cdot 7 \left\{ \begin{smallmatrix} 53 \cdot 1889 \\ 102059 \end{smallmatrix} \right.$	(6) $3^2 \cdot 5 \cdot 13 \left\{ \begin{smallmatrix} 11 \cdot 19 \\ 239 \end{smallmatrix} \right.$	

^{364b}Bibliotheca Math., (3), 14, 1915, 351-4.

(31) $3^2 \cdot 5 \cdot 13 \begin{Bmatrix} 11 \cdot 199 \\ 29 \cdot 79 \end{Bmatrix}$	(54) $3^2 \cdot 5^2 \begin{Bmatrix} 11 \cdot 59 \cdot 179 \\ 17 \cdot 19 \cdot 359 \end{Bmatrix}$	(13) $3^2 \cdot 5 \cdot 13 \cdot 19 \begin{Bmatrix} 29 \cdot 569 \\ 17099 \end{Bmatrix}$
(33) $3^2 \cdot 5 \cdot 13 \cdot 19 \begin{Bmatrix} 37 \cdot 1583 \\ 227 \cdot 263 \end{Bmatrix}$	(32) $3^2 \cdot 5 \cdot 13 \begin{Bmatrix} 19 \cdot 47 \\ 29 \cdot 31 \end{Bmatrix}$	(12) $3^2 \cdot 7^2 \cdot 11 \cdot 13 \begin{Bmatrix} 41 \cdot 461 \\ 19403 \end{Bmatrix}$
(41) $3^2 \cdot 7 \cdot 13 \cdot 23 \begin{Bmatrix} 11 \cdot 19 \cdot 367 \\ 79 \cdot 1103 \end{Bmatrix}$	(34) $3^2 \cdot 7^2 \cdot 13 \cdot 19 \begin{Bmatrix} 11 \cdot 220499 \\ 89 \cdot 29399 \end{Bmatrix}$	(false)
(30) $3^3 \cdot 5 \begin{Bmatrix} 7 \cdot 71 \\ 17 \cdot 31 \end{Bmatrix}$	(55) $3^3 \cdot 5 \begin{Bmatrix} 7 \cdot 21491 \\ 17 \cdot 23 \cdot 397 \end{Bmatrix}$	(42) $3^3 \cdot 5 \cdot 23 \begin{Bmatrix} 11 \cdot 19 \cdot 367 \\ 79 \cdot 1103 \end{Bmatrix}$
(11) $3^4 \cdot 5 \cdot 11 \begin{Bmatrix} 29 \cdot 89 \\ 2699 \end{Bmatrix}$	(56) $3^4 \cdot 7 \cdot 11^2 \cdot 19 \begin{Bmatrix} 47 \cdot 7019 \\ 389 \cdot 863 \end{Bmatrix}$	(57) $3^4 \cdot 7 \cdot 11^2 \cdot 19 \begin{Bmatrix} 53 \cdot 6959 \\ 179 \cdot 2087 \end{Bmatrix}$
(53) $3^5 \cdot 7^2 \cdot 13 \cdot 53 \begin{Bmatrix} 11 \cdot 211 \\ 2543 \end{Bmatrix}$	(58) $3^5 \cdot 7^2 \cdot 13 \cdot 19 \begin{Bmatrix} 47 \cdot 7019 \\ 389 \cdot 863 \end{Bmatrix}$	(59) $3^5 \cdot 7^2 \cdot 13 \cdot 19 \begin{Bmatrix} 53 \cdot 6959 \\ 179 \cdot 2087 \end{Bmatrix}$

Euler's final list of 61 pairs did not include the pairs α, β, γ , although he had obtained α four times in the body of his paper, viz., in (2), (3₁), (5₃); β twice in (3₁); γ in (2). Moreover, these three unlisted pairs occur as VIII, IX, and XIII among the 30 pairs in Euler's³⁶² earlier list, a fact noted on p. XXVI and p. LVIII of the Preface by P. H. Fuss and N. Fuss to Euler's Comm. Arith. Coll., who failed to observe that these three pairs occur in the text of Euler's present paper. Nor did these editors note that the fourth mentioned case of divergence between the two lists is due merely to the misprint^{364c} of 57 for 47 in (43) of the present list, so that the correctly printed pair XXVIII of the list of 30 is really this (43) and not a new pair, as supposed by them.

From the fact that Euler obtained in his posthumous tract⁹⁷ on amicable numbers the pairs α, β (once on p. 631 and again on p. 633 and finally on p. 635), the editors inferred, p. LXXXI of the Preface, that the tract differs in analysis from the long paper just discussed. But no new pairs are found, while the cases treated on pp. 631-2 are merely problems 1 and 2 of Euler's preceding paper. It is different with p. 634, where Euler started with two numbers like 71 and 5·11 which, by his table, have the same sum, 72, of divisors, and required a number a relatively prime to them such that $71a$ and $55a$ are amicable. The single condition is $72 \int a = (71 + 55)a$, whence $\int a : a = 7 : 4$. Thus a has the factor 4. If $a = 4b$, where b is odd, then $\int b = b = 1$, and the pair 284, 220 results. The case $a = 8b$ is impossible. This method was used in a special way by Kraft³⁶³ who limited the numbers from which one starts to a prime and a product of two primes.

In the Encyclopédie Sc. Math., I, 3₁, p. 59, note 320, it is stated that this posthumous tract contains four pairs not in Euler's list of 61, two pairs being those of Fermat³⁶⁴ and Descartes.³⁵⁵ But these were listed as (2) and (3) by Euler and were obtained by him in case (1₁) and attributed to Descartes.

E. Waring³⁶⁵ noted that $2^n x, 2^n yz$ are amicable if

$$x = \frac{2^n yz - 2^{n+1} + 1}{2^n - 1}, \quad z = 2^n - 1 + \frac{2^{2n}}{y - 2^n + 1},$$

where x, y, z are primes and $y - 2^n + 1$ divides 2^{2n} . He cited the first two such pairs of amicable numbers.

^{364c}G. Eneström, Bibliotheca Math., (3), 9, 1909, 263.

³⁶⁵Meditationes algebraicae, 1770, 201; ed. 3, 1782, 342-3.

The first three pairs were given in an anonymous work.³⁶⁶

In 1796, J. P. Gräson¹⁰⁰ (p. 87) gave the usual rule (1) leading to the three first known amicable pairs (verwandte Zahlen).

A. M. Legendre³⁶⁷ attributed the rule (1) to Descartes.

G. S. Klügel³⁶⁸ gave a process leading to the choice of P and Q , left arbitrary by Kraft.³⁶³ We have $A:a=R+1:PQ+R=2R-P-Q$. Thus $P+Q=\frac{1}{2}R(2A-a)-a/A$, while PQ is given by Kraft's second equation. Hence P and Q are the roots of a quadratic equation. For example, if $A=4$, then

$$8P, 8Q=R-7 \pm \sqrt{R^2-62R-63}.$$

The positive root of $x^2-62x-63=0$ lies between 60 and 61. Thus we try primes ≥ 61 for R , such that $R-7$ is divisible by 8. The first available R is 71, giving $P=11$, $Q=5$ and the amicable pair 220, 284. In general, the quantity $a^2R^2+2\beta R+\gamma$ under the radical sign can be made equal to the square of $aR+p$ (p arbitrary) by choice of R .

John Gough³⁶⁹ considered amicable numbers ax, ayz , where x, y, z are distinct primes not dividing a . Let q be the sum of the aliquot divisors of a . Then

$$a+q+qx=ayz, \quad x+1=(y+1)(z+1).$$

If $q \leq a/4$, the first gives $ayz < (1+x)a/4$, while $2y \cdot 2z > x+1$ by the second, Thus $q > a/4$. Let $a=r^n$, where r is a prime > 1 . Then $q=(a-1)/(r-1)$, which with $q > a/4$ implies $a(5-r) > 4$, $r=2$ or 3 . He proved that $r \neq 3$. whence $r=2$, the case treated by van Schooten.³⁵⁹

J. Struve¹⁰³ cited his Osterprogramm, 1815, on amicable numbers.

A. M. Legendre³⁷⁰ discussed the amicable numbers of the type (1_1) of Euler³⁶⁴ (with Euler's m, k replaced by $m-\mu, \mu$). Legendre noted that $r=2^{2m+k}(2^k+1)^2-1$ is of the form s^2-1 and hence composite, if k is even; also that, if $k=3$, $p=9 \cdot 2^{m+3}-1$, $q=9 \cdot 2^m-1$, one of which is of the form s^2-1 . He considered the new case $k=7$ and found for $m=1$ that $p=33023$, $q=257$, $r=8520191$, stating that if r be a prime we have the amicable numbers $2^8pq, 2^8r$. This is in fact the case.³⁷¹ For $k=1$, we have the ancient rule (1); he proved that for $n \leq 15$ it gives only the known three pairs of amicable numbers.

Paganini³⁷², at age 16, announced the amicable numbers $1184=2^5 \cdot 37$, $1210=2 \cdot 5 \cdot 11^2$, not in the list by Euler³⁶⁴, but gave no indication of the method of discovery.

³⁶⁶Encyclopédie méthodique...Amusemens des Sciences Math. et Phys., nouv. éd., Padoue, 1793, I, 116. Cf. Les amusemens math., Lille, 1749, 315.

³⁶⁷Théorie des nombres, 1798, 463.

³⁶⁸Math. Wörterbuch, 1, 1803, 246-252 [5, 1831, 55].

³⁶⁹New Series of the Math. Repository (ed., Th. Leybourn), vol. 2, pt. 2, 1807, 34-39. He cited Hutton's Math. Dict., article Amicable Numbers, taken from van Schooten³⁵⁹.

³⁷⁰Théorie des nombres, ed. 3, 1830, II, §472, p. 150. German transl. by H. Maser, Leipzig, 1893, II, p. 145.

³⁷¹Tchebychef, Jour. de Math., 16, 1851, 275; Werke, 1, 90. T. Pepin, Atti Acc. Pont. Nuovi Lincei, 48, 1889, 152-6. Kraitichik, Sphinx-Oedipe, 6, 1911, 92. Also by Lehmer's Factor Table or Table of Primes.

³⁷²B. Nicolò I. Paganini, Atti della R. Accad. Sc. Torino, 2, 1866-7, 362. Cf. Cremona's Ital. transl. of Baltzer's Mathematik, pt. III.

P. Seelhoff³⁷³ treated Euler's³⁶⁴ problems 1 and 2 by Euler's methods (though the contrary is implied), and gave about 20 pairs of amicable numbers due to Euler, with due credit for only three pairs. The only new pairs (pp. 79, 84, 89) are

$$3^{27} 2^{13} \cdot 19 \cdot 23 \begin{cases} 83 \cdot 1931 \\ 162287 \end{cases} \quad 2^6 \begin{cases} 139 \cdot 863 \\ 167 \cdot 719. \end{cases}$$

E. Catalan³⁷⁴ stated empirically that if n_1 is the sum of the divisors $< n$ of n , and n_2 is the sum of the divisors $< n_1$ of n_1 , etc., then n, n_1, n_2, \dots have a limit λ , where λ is unity or a perfect number.

J. Perrott³⁷⁵ [Perott] noted that there is no limit for $n = 220$, since

$$n_1 = n_3 = \dots = 284, \quad n_2 = n_4 = \dots = 220.$$

H. LeLasseur³⁷⁶ found that for $n < 35$ the numbers (1) are all odd primes, and hence give amicable numbers, only when $n = 2, 4, 7$.

Josef Bezdiček³⁷⁷ gave a translation into Bohemian of Euler,³⁶⁴ without credit to Euler, and a table of 65 pairs of amicable numbers.

Aug. Haas³⁷⁸ proved that, if M and N are amicable numbers,

$$1/\Sigma \frac{1}{m} + 1/\Sigma \frac{1}{n} = 1,$$

where m and n range over all divisors of M and N , respectively. For, $\Sigma m = \Sigma n = M + N$, so that

$$\Sigma \frac{1}{m} = \frac{\Sigma m}{M} = \frac{M+N}{M}, \quad \Sigma \frac{1}{n} = \frac{\Sigma n}{N} = \frac{M+N}{N}.$$

If $M = N$, N is perfect and the result becomes that of Catalan.¹⁴⁵

A. Cunningham³⁷⁹ considered the sum $s(n)$ of the divisors $< n$ of n and wrote $s^2(n)$ for $s\{s(n)\}$, etc. For most numbers, $s^k(n) = 1$ when k is sufficiently large. There is a small class of perfect and amicable numbers, and a small class of numbers n (even when $n < 1000$) for which $s^k(n)$ increases beyond the practical power of calculation [cf. Catalan³⁷⁴].

A. Gérardin³⁸⁰ proved that the only pairs $2^2 \cdot 5x$, $2^2 yz$ of amicable numbers, where x, y, z are odd primes, are Euler's (α) , (β) ; the only pairs $2^4 \cdot 23x$, $2^4 yz$ are Euler's (17), (19), (20). He cited the Exercices d'arithmétique of Fitz-Patrick and Chevrel; also Dupuis' Table de logarithmes, which gives 24 pairs of amicable numbers.

Gérardin³⁸¹ proved that the only pair $8xy$, $32z$ is Euler's (60). He made an incomplete examination of $16 \cdot 53x$, $16yz$, but found no new pairs.

³⁷³Archiv Math. Phys., 70, 1884, 75-89.

³⁷⁴Bull. Soc. Math. France, 16, 1887-8, 129. Mathesis, 8, 1888, 130.

³⁷⁵Ibid., 17, 1888-9, 155-6.

³⁷⁶Lucas, Théorie des nombres, 1, 1891, 381.

³⁷⁷Casopis mat. a fys., Praze (Prag), 25, 1896, 129-142, 209-221.

³⁷⁸Ibid., 349-350.

³⁷⁹Proc. London Math. Soc., 35, 1902-3, 40.

³⁸⁰Mathesis, 6, 1906, 41-44.

³⁸¹Sphinx-Oedipe, Nancy, 1906-7, 14-15, 53.

Gérardin³⁸² proved that the three numbers (1) with $n = m + 2$ are not all primes if $34 < m \leq 60$, the cases $m = 38$ and 53 not being decided. Replacing m by $m + 1$ and k by $2g + 1$ in case (1₁) of Euler³⁶⁴, we get the pair $2^n pq$, $2^n r$, where $n = m + 2g + 2$,

$$p = 2^{m+2g+2}P - 1, \quad q = 2^{m+1}P - 1, \quad r = 2^{2m+2g+3}P^2 - 1,$$

with $P = 2^{2g+1} + 1$. For $g = 0$, we have the case (1) just mentioned; all values $m \leq 200$ are excluded except $m = 38, 74, 98, 146, 149, 182, 185, 197$. The case $g = 1$ is excluded since y or z is a difference of two squares. For $g = 2$, all values $m \leq 60$ are excluded except $m = 29, 34, 37, 49$. For $g = 3$, all values < 100 are excluded except $m = 8, 15, 23, 92$.

O. Meissner,³⁸³ using the notation of Cunningham,³⁷⁹ noted that n and $s(n)$ are amicable if $s^2(n) = n$ and raised the question of the existence of numbers n for which $s^k(n) = n$ for $k \geq 3$, so that $n, s(n), \dots, s^{k-1}(n)$ would give amicable numbers of higher order. He asked if the repetition of the operation s , a finite number (k) of times always leads to a prime, a perfect or amicable number; also if k increases with n to infinity. On these questions, see Dickson³⁸⁶ and Poulet.³⁸⁷

A. Gérardin³⁸⁴ stated that the only values $n < 200$ for which the numbers (1) are all primes are the three known to Descartes.

L. E. Dickson³⁸⁵ obtained the two new pairs of amicable numbers

$$2^4 \cdot 12959 \cdot 50231, \quad 2^4 \cdot 17 \cdot 137 \cdot 262079; \quad 2^4 \cdot 10103 \cdot 735263, \quad 2^4 \cdot 17 \cdot 137 \cdot 2990783,$$

by treating the type $16pq$, $16 \cdot 17 \cdot 137r$, where p, q, r are distinct odd primes. These are amicable if and only if

$$p = m + 9935, \quad q = n + 9935, \quad r = 4(m + n) + 88799, \quad mn = 2^7 3^4 7 \cdot 23 \cdot 73.$$

Although Euler³⁶⁴ mentioned this type (3₃) in §95, he made no discussion of it since r always exceeds the limit 100000 of the table of primes accessible to him. An examination of the 120 distinct cases led only to the above two amicable pairs.

Dickson³⁸⁶ proved that there exist only five pairs of amicable numbers in which the smaller number is < 6233 , viz., (1), (α), (β), (60) in Euler's³⁶⁴ table, and Paganini's³⁷² pair. In the notation of Cunningham,³⁷⁹ the chain $n, s(n), s^2(n), \dots$ is said to be of period k if $s^k(n) = n$. The empirical theorem of Catalan³⁷⁴ is stated in the corrected form that every non-periodic chain contains a prime and verified for a wide range of values of n . In particular, if $n < 6233$, there is no chain of period 3, 4, 5, or 6. For k odd and > 1 , there is no chain an_1, an_2, \dots, an_k of period k in which n_1, \dots, n_k have no common factor and each n_j is prime to $a > 1$.

³⁸²Sphinx-Oedipe, 1907-8, 49-56, 65-71; some details are inaccurate, but the results correct.

³⁸³Archiv Math. Phys., (3), 12, 1907, 199; Math.-Naturw. Blätter, 4, 1907, 86 (for $k = 3$).

³⁸⁴Assoc. franç. avanc. sc., 37, 1908, 36-48; l'intermédiaire des math., 1909, 104.

³⁸⁵Amer. Math. Monthly, 18, 1911, 109.

³⁸⁶Quart. Jour. Math., 44, 1913, 264-296.

P. Poulet³⁸⁷ discovered the chain of period five,

$$n = 12496 = 2^4 \cdot 11 \cdot 71, \quad s(n) = 2^4 \cdot 19 \cdot 47, \quad s^2(n) = 2^4 \cdot 967, \quad s^3(n) = 2^3 \cdot 23 \cdot 79, \\ s^4(n) = 2^3 \cdot 1783,$$

with $s^5(n) = n$; and noted that 14316 leads a chain of 28 terms.

GENERALIZATIONS OF AMICABLE NUMBERS.

Daniel Schwenter⁵² noted in 1636 that 27 and 35 have the same sum of aliquot parts. Kraft³⁶³ noted in 1749 that this is true of the pairs 45, 3·29; 39, 55; 93, 145; and 45, 13·19. In 1823, Thomas Taylor¹⁰² called two such numbers imperfectly amicable, citing the pairs 27, 35; 39, 55; 65, 77; 51, 91; 95, 119; 69, 133; 115, 187; 87, 247. George Peacock⁴⁰⁰ used the same term.

E. B. Escott⁴⁰¹ asked if there exist three or more numbers such that each equals the sum of the [aliquot] divisors of the others.

A. Gérardin⁴⁰² called numbers with the same sum of aliquot parts *nombres associés*, citing 6 and 25; 5·19, 7·17, and 11·13, and many more sets. An equivalent definition is that the n numbers be such that the product of $n-1$ by the sum of the aliquot divisors of any one of them shall equal the sum of the aliquot divisors of the remaining $n-1$ numbers.

L. E. Dickson⁴⁰³ defined an amicable triple to be three numbers such that the sum of the aliquot divisors of each equals the sum of the remaining two numbers. After developing a theory analogous to that by Euler³⁶⁴ for amicable numbers, Dickson obtained eight sets of amicable triples in which two of the numbers are equal, and two triples of distinct numbers:

$$\begin{array}{llll} 293 \cdot 337a, & 5 \cdot 16561a, & 99371a & (a = 2^5 \cdot 3 \cdot 13), \\ 3 \cdot 89b, & 11 \cdot 29b, & 359b & (b = 2^{14} \cdot 5 \cdot 19 \cdot 31 \cdot 151). \end{array}$$

³⁸⁷L'intermédiaire des math., 25, 1918, 100-1.

⁴⁰⁰Encyclopaedia Metropolitana, London, I, 1845, 422.

⁴⁰¹L'intermédiaire des math., 6, 1899, 152.

⁴⁰²Sphinx-Oedipe, 1907-8, 81-83.

⁴⁰³Amer. Math. Monthly, 20, 1913, 84-92.

CHAPTER II.

FORMULAS FOR THE NUMBER AND SUM OF DIVISORS, PROBLEMS OF FERMAT AND WALLIS.

FORMULA FOR THE NUMBER OF THE DIVISORS OF A NUMBER.

Cardan¹ stated that a product P of k distinct primes has $1+2+2^2+\dots+2^{k-1}$ aliquot parts (divisors $< P$).

Michael Stifel² proved this rule and found³ the number of divisors of $2^4 3^5 5^2 P$, where $P=7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$, by first noting that there are $1+2+\dots+64$ divisors $< P$ of P according to Cardan's rule and hence 128 divisors of P . The factor 5^2 gives rise to $128+128$ more divisors, so that we now have 384 divisors. The factor 3^3 gives 3.384 more, so that we have 1536. Then the factor 2^4 gives 4,1536 more.

Mersenne⁴ asked what number has 60 divisors; since $60=2 \cdot 2 \cdot 3 \cdot 5$, subtract unity from each prime factor and use the remainders 1, 1, 2, 4 as exponents; thus $3^2 \cdot 2^4 \cdot 7 \cdot 5 = 5040$ (so much lauded by Plato) has 60 divisors. It is no more difficult if a large number of aliquot parts is desired.

I. Newton⁵ found all the divisors of 60 by dividing it by 2, the quotient 30 by 2, and the new quotient 15 by 3. Thus the prime divisors are 1, 2, 2, 3, 5. Their products by twos give 4, 6, 10, 15. The products by threes give 12, 20, 30. The product of all is 60. The commentator J. Castillionei, of the 1761 edition, noted that the process proves that the number of all divisors of $a^m b^n \dots$ is $(m+1)(n+1) \dots$ if a, b, \dots are distinct primes.

Frans van Schooten⁶ devoted pp. 373-6 to proving that a product of k distinct primes has $2^k - 1$ aliquot parts and made a long problem (p. 379) of that to find the number of divisors of a given number. To find (pp. 380-4) the numbers having 15 aliquot parts, he factored $15+1$ in all ways and subtracted unity from each factor, obtaining $abcd$, a^3bc , a^3b^3 , a^7b , a^{15} . By comparing the arithmetically least numbers of these various types, he found (pp. 387-9) the least number having 15 aliquot parts.

John Kersey⁷ cited the long rule of van Schooten to find the number of aliquot parts of a number and then gave the simple rule that $a_1^{e_1} \dots a_n^{e_n}$ has $(e_1+1) \dots (e_n+1)$ divisors in all if a_1, \dots, a_n are distinct primes.

John Wallis⁸ gave the last rule. To find a number with a prescribed number of divisors, factor the latter number in all possible ways; if the

¹Practica Arith. & Mensurandi, Milan, 1537; Opera, IV, 1663.

²Arithmetica Integra, Norimbergae, 1544, lib. 1, fol. 101.

³Stifel's posthumous manuscript, fol. 12, preceding the printed text of Arith. Integra; cf. E.

Hoppe, Mitt. Math. Gesell. Hamburg, 3, 1900, 413.

⁴Cogitata Physico Math., II, Hydraulica Pneumatica, Preface, No. 14, Paris, 1644. (Quoted by Winsheim, Novi Comm. Ac. Petrop., II, ad annum 1749, Mem., 68-99). Also letter from Mersenne to Torricello, June 24, 1644, Bull. Bibl. Storia Sc. Mat., 8, 1875, 414-5.

⁵Arithmetica Universalis, ed. 1732, p. 37; ed. 1761, I, p. 61. De Inventionem Divisorum.

⁶Exercitationum Math., Lugd. Batav., 1657.

⁷The Elements of Algebra, London, vol. 1, 1673, p. 199.

⁸A Treatise of Algebra, London, 1685, additional treatise, Ch. III.

factors are r, s, \dots , the required number is $p^{r-1}q^{s-1}\dots$, where p, q, \dots are any distinct primes. When the number of divisors is odd, the number itself is a square, and conversely. The number of ways $N = a^\alpha b^\beta \dots$ can be expressed as a product of two factors is $k = \frac{1}{2}(\alpha+1)(\beta+1)\dots$ or $\frac{1}{2} + k$, according as N is not or is a square.

Jean Prestet⁹ noted that a product of k distinct primes has 2^k divisors, while the n th power of a prime has $n+1$ divisors. The divisors of $a^2b^3c^2$ are the 12 divisors of a^2b^3 , their products by c and by c^2 , the general rule not being stated explicitly.

Pierre Rémond de Montmort¹⁰ stated in words that the number of divisors of $a_1^{e_1} \dots a_n^{e_n}$ is $(e_1+1) \dots (e_n+1)$ if the a 's are distinct primes.

Abbé Deidier¹¹ noted that a product of k distinct primes has

$$1 + k + \binom{k}{2} + \binom{k}{3} + \dots$$

divisors, treating the problem as one on combinations (but did not sum the series and find 2^k). To find the number of divisors of $2^43^35^2$ he noted that five are powers of 2 (including unity). Since there are three divisors of 3^3 , multiply 5 by 3 and add 5, obtaining 20. In view of the two divisors of 5^2 , multiply 20 by 2 and add 20. The answer is 60.

E. Waring¹² proved that the number of divisors of $a^m b^n \dots$ is $(m+1)(n+1) \dots$ if a, b, \dots are distinct primes, and that the number is a square if the number of its divisors is odd.

E. Lionnet¹³ proved that if a, b, c, \dots are relatively prime in pairs, the number of divisors of $abc \dots$ equals the product of the number of divisors of a by the number for b , etc. According as a number is a square or not, the number of its divisors is odd or even.

T. L. Pujo¹⁴ noted the property last mentioned.

Emil Hain¹⁵ derived the last theorem from $a^m = (t_1 \dots t_m)^2$, where t_1, \dots, t_m denote the divisors of a .

A. P. Minin¹⁶ determined the smallest integer with a given number of divisors.

G. Fontené¹⁷ noted that, if $2^\alpha 3^\beta \dots m^\mu n^\nu$ ($\alpha \geq \beta \geq \dots \geq \mu \geq \nu$) is the least number with a given number of divisors, then $\nu+1$ is a prime, and $\mu+1$ is a prime except for the least number $2^3 3$ having eight divisors.

FORMULA FOR THE SUM OF THE DIVISORS OF A NUMBER.

R. Descartes,²¹ in a manuscript, doubtless of date 1638, noted that, if p is a prime, the sum of the aliquot parts of p^n is $(p^n - 1)/(p - 1)$. If b is the

⁹Nouv. Elemens des Math., Paris, 1689, vol. 1, p. 149.

¹⁰Essay d'analyse sur les jeux de hazard, ed. 2, Paris, 1713, p. 55. Not in ed. 1, 1708.

¹¹Suite de l'arithmétique des géomètres, Paris, 1739, p. 311.

¹²Medit. Algebr., 1770, 200; ed. 3, 1782, 341.

¹³Nouv. Ann. Math., (2), 7, 1868, 68-72.

¹⁴Les Mondes, 27, 1872, 653-4.

¹⁵Archiv Math. Phys., 55, 1873, 290-3.

¹⁶Math. Soc. Moscow (in Russian), 11, 1883-4, 632.

¹⁷Nouv. Ann. Math., (4), 2, 1902, 288; proof by Chalde, 3, 1903, 471-3.

²¹"De partibus aliquotis numerorum," Opuscula Posthuma Phys. et Math., Amstelodami, 1701, p. 5; Oeuvres de Descartes (ed. Tannery and Adams, 1897-1909), vol. 10, pp. 300-2.

sum of the aliquot parts of a , the sum of the aliquot parts of ap is $bp + a + b$. If b is the sum of the aliquot parts of a and if x is prime to a , the sum of the aliquot parts of ax^n is

$$\frac{bx^{n+1} + ax^n - a - b}{x - 1} \quad \left[= (b + a) \left(\frac{x^{n+1} - 1}{x - 1} \right) - ax^n \right].$$

Descartes²² stated a result which may be expressed by the formula

$$(1) \quad \sigma(nm) = \sigma(n)\sigma(m) \quad (n, m \text{ relatively prime}),$$

where $\sigma(n)$ is the sum of the divisors (including 1 and n) of n . Here he solved $n : \sigma(n) = 5 : 13$. Thus n must be divisible by 5. Enter 5 in column A and $\sigma(5) = 6$ in column B . Then enter the factor 2 in column A and $\sigma(2) = 3$ in column B . Having two threes in column B , we enter 9 in column A and $\sigma(9) = 13$ in B . Every number except 13 in column B is in column A . Hence the product $5 \cdot 2 \cdot 9 = 90$ is a solution n . Next, to solve $n : \sigma(n) = 5 : 14$, we enter also 13 in column A and 14 in B , and obtain the solution $90 \cdot 13$. If n is a perfect number, $5n : \sigma(5n) = 5 : 12$ and, if $n \neq 6$, $15n : \sigma(15n) = 5 : 16$.

A	B
5	2·3
2	3
9	13

Descartes²³ stated that he possessed a general rule [illustrated above] for finding numbers having any given ratio to the sum of their aliquot parts.

Fermat²⁴ had treated the same problem. Replying to Mersenne's remark that the sum of the aliquot parts of 360 bears to 360 the ratio 9 to 4, Fermat²⁵ noted that 2016 has the same property.

John Wallis²⁶ noted that Frenicle knew formula (1).

Wallis²⁷ knew the formula

$$(2) \quad \sigma(a^\alpha b^\beta \dots) = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \dots$$

Thus these formulæ were known before 1685, the date set by Peano,²⁸ who attributed them to Wallis.⁵²

G. W. Kraft²⁹ noted that the method of Newton⁵ shows that the sum of the divisors of a product of distinct primes P, \dots, S is $(P+1) \dots (S+1)$. He gave formula (1) and also (2), a formula which Cantor³⁰ stated had probably not earlier been in print. To find a number the sum of whose divisors is a square, Kraft took PA , where P is a prime not dividing A . If $\sigma(A) = a$, then $\sigma(PA) = (P+1)a$ will be the square of $(P+1)B$ if $P =$

²²"De la façon de trouver le nombres de parties aliquotes in ratione data," manuscript Fonds-français, nouv. acquisitions, No. 3280, ff. 156-7, Bibliothèque Nationale, Paris. Published by C. Henry, Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 713-5.

²³Oeuvres, 2, p. 149, letter to Mersenne, May 27, 1638.

²⁴Oeuvres de Fermat, 2, top of p. 73, letter to Roberval, Sept. 22, 1636.

²⁵Oeuvres, 2, 179, letter to Mersenne, Feb. 20, 1639.

²⁶Commercium Epistolicum, letter 32, April 13, 1658; French transl. in Oeuvres de Fermat, 3, 553.

²⁷Commercium Epist., letter 23, March, 1658; Oeuvres de Fermat, 3, 515-7.

²⁸Formulaire Math., 3, Turin, 1901, 100-1.

²⁹Novi Comm. Ac. Petrop., 2, 1751, ad annum 1749, 100-109.

³⁰Geschichte Math., 3, 595; ed. 2, 616.

$a/B^2 - 1$; for $A = 14$, take $B = 2$, whence $P = 5$. Again, the sum of the aliquot parts of $3P^2$ is $(2+P)^2$. The numbers AP and BPQ have the same sum of divisors if $a(P+1) = b(P+1)(Q+1)$, i. e., if $Q = a/b - 1$; taking $a = 24$, $b = 6$, we have $Q = 3$, a prime, $A = 14$, $B = 5$ (by his table of the sum of the divisors of $1, \dots, 150$); this problem had been solved otherwise by Wolff.³¹

L. Euler³² gave a table of the prime factors of $\sigma(p)$, $\sigma(p^2)$, and $\sigma(p^3)$ for each prime $p < 1000$; also those of $\sigma(p^a)$ for various a 's for $p \leq 23$ (for instance, $a \leq 36$ when $p = 2$). He proved formulas (1) and (2) here and in his³³ posthumous tract, where he noted (p. 514) all the cases in which $\sigma(n) = \sigma(m) \leq 60$.

E. Waring¹² proved formula (2). He³⁴ noted that if $P = a^m b^n \dots$ and $Q = a^x b^y \dots$, where $m - a, n - \beta, \dots$ are large, then $\sigma(PQ)/\sigma(P)$ is just greater than Q . If $A = (l-1)!$, $\sigma(lA)/\sigma(A) \leq l+1$. If $a^x b^y \dots = A$ and $(x+1)(y+1) \dots$ is a maximum, then $a^{x+1} = b^{y+1} = \dots$. For a, b, \dots distinct primes, $\sigma(A)$ is not a maximum. He cited numbers with equal sums of divisors: 6 and 11, 10 and 17, 14 and 15 and 23.

L. Kronecker³⁵ derived the formulas for the number and sum of the divisors of an integer by use of infinite series and products.

E. B. Escott³⁶ listed integers whose sum of divisors is a square.

PROBLEMS OF FERMAT AND WALLIS ON SUMS OF DIVISORS.

Fermat⁴⁰ proposed January 3, 1657, the two problems: (i) Find a cube which when increased by the sum of its aliquot parts becomes a square;* for example, $7^3 + (1+7+7^2) = 20^2$. (ii) Find a square which when increased by the sum of its aliquot parts becomes a cube.

John Wallis⁴¹ replied that unity is a solution of both problems and proposed the new problem: (iii) Find two squares, other than 16 and 25, such that if each is increased by the sum of its aliquot parts the resulting sums are equal.

Brouncker⁴² gave $1/n^6$ and $343/n^6$ as solutions (!) of problem (i).

³¹Elementa Analyseos, Cap. 2, prob. 87.

³²Opuscula varii argumenti, 2, Berlin, 1750, p. 23; Comm. Arith., 1, 102 (p. 147 for table to 100). Opera postuma, I, 1862, 95-100. F. Rudio, Bibl. Math., (3), 14, 1915, 351, stated that there are fully 15 errors.

³³Comm. Arith., 2, 512, 629. Opera postuma, I, 12-13.

³⁴Meditationes Algebr., ed. 3, 1782, 343. (Not in ed. of 1770.)

³⁵Vorlesungen über Zahlentheorie, I, 1901, 265-6.

³⁶Amer. Math. Monthly, 23, 1916, 394.

*Erroneously given as "cube" in the French tr., Oeuvres de Fermat, 3, 311.

⁴⁰Oeuvres, 2, 332, "premier défi aux mathématiciens;" also, pp. 341-2, Fermat to Digby, June 6, 1657, where 7^3 is said to be not the only solution. These two problems by Fermat were quoted in a letter by the Astronomer Jean Hévélius, Nov. 1, 1657, published by C. Henry, Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 683-5, along with extracts from the *Commercium Epistolicum*. Cf. G. Wertheim, Abh. Geschichte Math., 9, 1899, 558-561, 570-2 (=Zeitschr. Math. Phys., 44, Suppl. 14).

⁴¹Commercium Epistolicum de Wallis, Oxford, 1658; Wallis, Opera, 2, 1693. Letter II, from Wallis to Brouncker, Mar. 17, 1657; letter XVI, Wallis to Digby, Dec. 1, 1657. Oeuvres de Fermat, 3, 404, 414, 427, 482-3, 503-4, 513-5.

⁴²Commercium, letter IX, Wallis to Digby; Fermat's Oeuvres, 3, 419.

Frenicle⁴³ expressed his astonishment that experienced mathematicians should not hesitate to present, for the third time, unity as a solution.

Wallis⁴⁴ tabulated $\sigma(x^3)$ for each prime $x < 100$ and for low powers of 2, 3, 5, and then excluded those primes x for which $\sigma(x^3)$ has a prime factor not occurring elsewhere in the table. By similar eliminations and successive trials, he was led to the solutions⁴⁵ of (i):

$$a = 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 41 \cdot 47, \quad b = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 41 \cdot 47; \quad 7a, 7b,$$

adding that they are identical with the four numbers given by Frenicle.⁴⁶ Note that $\sigma(a)$ is the square of $2^3 3^{25} \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 61$, while $\sigma(b)$ is the square of $2^7 3^{25} \cdot 7 \cdot 13 \cdot 17 \cdot 29$. Wallis⁴⁷ gave the further solutions of $\sigma(x^3) = y^2$:

$$\begin{array}{ll} x = 17 \cdot 31 \cdot 47 \cdot 191, & y = 2^{10} 3^{25} \cdot 13 \cdot 17 \cdot 29 \cdot 37, \\ 2 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 31 \cdot 41 \cdot 191, & 2^{12} 3^5 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 29^2 \cdot 37, \\ 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 41 \cdot 191, & 2^{13} 3^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29^2 \cdot 37 \cdot 61, \end{array}$$

and the products of each x by 7.

Wallis⁴⁸ gave solutions of his problem (iii):

$$\begin{array}{ll} 2^3 \cdot 37, 2 \cdot 19 \cdot 29; & 2^2 \cdot 3 \cdot 11 \cdot 19 \cdot 37, 2^3 \cdot 7 \cdot 29 \cdot 67; \\ 29 \cdot 67, 2 \cdot 3 \cdot 5 \cdot 37; & 2^3 \cdot 7 \cdot 29 \cdot 67, 3 \cdot 5 \cdot 11 \cdot 19 \cdot 37. \end{array}$$

Frenicle⁴⁹ gave 48 solutions of Wallis' problem (iii), including $2 \cdot 163 \cdot 11 \cdot 37$; $3 \cdot 11 \cdot 19$, $7 \cdot 107$; $2 \cdot 5 \cdot 151$, $3^3 \cdot 67$; also 83 sets of three squares having the same sum of divisors, for example, the squares of

$$2^{21} \cdot 11 \cdot 37 \cdot 151, \quad 3^3 \cdot 67 \cdot 163, \quad 5 \cdot 11 \cdot 37 \cdot 151, \quad \sigma = 3^{27} \cdot 19 \cdot 31 \cdot 67 \cdot 1093;$$

also various such sets of n squares (with prime factors < 500) for $n \leq 19$, for example, the squares of ac , ad , $4bd$, $4bc$, $5bd$, and $5bc$, where

$$a = 2 \cdot 5 \cdot 29 \cdot 47 \cdot 67 \cdot 139, \quad b = 13 \cdot 37 \cdot 191 \cdot 359, \quad c = 7 \cdot 107, \quad d = 3 \cdot 11 \cdot 19.$$

Frans van Schooten⁵⁰ made ineffective attempts to solve problems (i), (ii).

Frenicle⁵¹ gave the solution

$$x = 2^2 \cdot 5 \cdot 7 \cdot 11 \cdot 37 \cdot 67 \cdot 163 \cdot 191 \cdot 263 \cdot 439 \cdot 499, \quad y = 3^{27} \cdot 13 \cdot 19 \cdot 31^2 \cdot 67 \cdot 109$$

of problem (ii), $\sigma(x^2) = y^3$; also a new solution of $\sigma(x^3) = y^2$:

$$x = 2^5 \cdot 5 \cdot 7 \cdot 31 \cdot 73 \cdot 241 \cdot 243 \cdot 467, \quad y = 2^{12} 3^{25} \cdot 11 \cdot 13^2 \cdot 17 \cdot 37 \cdot 41 \cdot 113 \cdot 193 \cdot 257.$$

⁴³Letter XXII, to Digby, Feb. 3, 1658. Cf. Leibnitii et Bernoullii Commercium philos. et math., I, 1795, 263, letter from Johann Bernoulli to Leibniz, Apr. 3, 1697.

⁴⁴Letter XXIII, to Digby, Mar. 14, 1658.

⁴⁵The same tentative process for finding this solution a was given by E. Waring, *Meditationes Algebraicae*, 1770, pp. 216–7; ed. 3, 1782, 377–8. The solution $b = 751530$ was quoted by Lucas, *Théorie des nombres*, 1891, 380, ex. 3.

⁴⁶*Solutio duorum problematum circa numeros cubos*... 1657, dedicated to Digby [lost work]. See *Oeuvres de Fermat*, p. 2. 434, Note; Wallis.⁵²

⁴⁷Letter XXVIII, March 25, 1658; Wallis, *Opera*, 2, 814; Wallis⁵².

⁴⁸Letter XXIX, Mar. 29, 1658; Wallis⁵².

⁴⁹Letter XXXI, Apr. 11, 1658.

⁵⁰Letter XXXIII, Feb. 17, 1657 and Mar. 18, 1658.

⁵¹Letter XLIII, May 2, 1658.

Wallis⁵² for use in problem (ii) gave a table showing the sum of the divisors of the square of each number < 500 . Excluding numbers in whose divisor sum occurs a prime entering the table only once or twice, there are left the squares of 2, 4, 8, 3, 5, 7, 11, 19, 29, 37, 67, 107, 163, 191, 263, 439, 499. By a very long process of exclusion he found only two solutions within the limits of the table, viz., Frenicle's⁵¹ and

$$\sigma\{(7 \cdot 11 \cdot 29 \cdot 163 \cdot 191 \cdot 439)^2\} = \{3 \cdot 7 \cdot 13 \cdot 19 \cdot 31 \cdot 67\}^3.$$

Jacques Ozanam⁵³ stated that Fermat had proposed the problem to find a square which with its aliquot parts makes a square (giving 81 as the answer) and the problem to find a square whose aliquot parts make a square. For the latter, Ozanam found 9 and 2401, whose aliquot parts make 4 and 400, and remarked that he did not believe that Fermat ever solved these questions, although he proposed them as if he knew how.

Ozanam⁵⁴ noted that the sum of $961 = 31^2$ and its aliquot parts 1 and 31 is 993, which equals the sum of the aliquot parts of $1156 = 34^2$. As examples of two squares with equal total sums of divisors [Wallis' problem (iii)], he cited 16 and 25, 326^2 and 407^2 , while others may be derived by multiplying these by an odd square not divisible by 5. The sum of all the divisors of 9^2 is 11^2 , that of 20^2 is 31^2 . The numbers 99 and 63 have the property that the sum 57 of the aliquot parts of 99 exceeds the sum 41 of the aliquot parts of 63 by the square 16; similarly for 325 and 175.

E. Lucas⁵⁵ noted that the problem to find all integral solutions of

$$(1) \quad 1 + x + x^2 + x^3 = y^2$$

is equivalent to the solution of the system

$$(2) \quad 1 + x = 2u^2, \quad 1 + x^2 = 2v^2, \quad y = 2uv,$$

and stated that the complete solution is given by that of $2v^2 - x^2 = 1$.

E. Gerono⁵⁶ proved that the only solutions of (1) are

$$(x, y) = (-1, 0), \quad (0, \pm 1), \quad (1, \pm 2), \quad (7, \pm 20).$$

E. Lucas⁵⁷ stated that there is an infinitude of solutions of Fermat's problem (i); the least composite solution is the cube of $2 \cdot 3 \cdot 5 \cdot 13 \cdot 41 \cdot 47$, the sum of whose divisors is the square of $2^7 3^2 5^2 7 \cdot 13 \cdot 17 \cdot 29$. [This solution was given by Frenicle.⁴⁶] For the case of a prime, the problem becomes (1).

A. S. Bang⁵⁸ gave for problem (i) the first of the three answers by Wallis;⁴⁷ for (ii), $\sigma(43098^2) = 1729^3$; for (iii), $29 \cdot 67$, $2 \cdot 3 \cdot 5 \cdot 37$ of Wallis⁴⁸ and the first two by Frenicle;⁴⁹ all without references.

⁵²A Treatise of Algebra, 1685, additional treatises, Ch. IV.

⁵³Letter to De Billy, Nov. 1, 1677, published by C. Henry, Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 519. Reprinted in Oeuvres de Fermat, 4, 1912, p. 140.

⁵⁴Récréations Mathématiques et Phys., new ed., 1723, 1724, 1735, etc., Paris, I, 41–43.

⁵⁵Nouv. Corresp. Math., 2, 1876, 87–8.

⁵⁶Nouv. Ann. Math., (2), 16, 1877, 230–4.

⁵⁷Bull. Bibl. Storia Sc. Mat. e Fis., 10, 1877, 287.

⁵⁸Nyt Tidsskrift for Mat., 1878, 107–8; on problems in 1877, 180.

E. Fauquembergue,⁵⁹ after remarking that (1) is equivalent to the system (2), cited Fermat's⁶⁰ assertion that the first two equations (2) hold only for $x=7$ [aside from the evident solutions $x=\pm 1, 0$], which has been proved by Genocchi.⁶¹

H. Brocard⁶² thought that Fermat's assertion that 7^3 is not the only solution of problem (i) implied a contradiction with Genocchi.⁶¹ G. Vacca (*ibid.*, p. 384) noted the absence of contradiction as (i) leads to equation (1) only if x be a prime.

C. Moreau⁶³ treated the equation, of type (1),

$$x^4+x^3+x^2+x+1=y^2.$$

While he used the language of extracting the square root of $X=x^4+\dots$ written to the base x , he in effect put $X=(x^2+a)^2$, $0<a<x$. Then $a^2=x+1$, $2ax^2=x^3+x^2$, whence $2a=a^2$, $a=2$, $x=3$, $y=11$.

E. Lucas⁶⁴ stated that $(x^5+y^5)/(x+y)=z^2$ has the solutions

$$(3, -1, 11), (8, 11, 101), (123, 35, 13361), \dots$$

Moret-Blanc⁶⁵ gave also the solutions $(0, 1, 1)$, $(1, 1, 1)$.

E. Landau⁶⁶ proved that the equation

$$\frac{x^n-1}{x-1}=y^2$$

is impossible in integers (aside from $x=0$, $y=\pm 1$) for an infinitude of values of n , viz., for all n 's divisible by 3 such that the odd prime factors of $n/3$, if any, are all of the form $6v-1$ (the least such n being 6). For, setting $n=3m$, we see that y^2 is the product of x^2+x+1 and $F=x^{3m-3}+\dots+x^3+1$. These two factors are relatively prime since $x^3\equiv 1$ gives $F\equiv m \pmod{x^2+x+1}$. Hence x^2+x+1 is a square, which is impossible for $x\neq 0$ since it lies between x^2 and $(x+1)^2$.

Brocard⁶² had noted the solution $x=1$, $y=m$, if $n=m^2$.

A. Gérardin⁶⁷ obtained six new solutions of problem (i):

$x=2.47.193.239.701,$	$y=2^7.3^3.5^3.13^3.17.97.149.$
$x=2.5.23.41.83.239,$	$y=2^8.3^3.5^2.7.13^3.29.53.$
$x=3.13.23.47.83.239,$	$y=2^{11}.3^2.5^3.7.13^3.17.53.$
$x=2.3.13.23.83.193.701,$	$y=2^8.3^3.5^4.7.13.17.53.97.149.$
$x=3.5.13.41.193.239.701,$	$y=2^9.3^3.5^3.7.13^3.17.29.97.149.$
$x=2.5.13.43.191.239.307,$	$y=2^{13}.3^2.5^3.11^2.17.29.37.53.113.197.241.257.$

Also $\sigma(N^2)=S^2$ for $N=3\cdot 7\cdot 11\cdot 29\cdot 37$, $S=3\cdot 7\cdot 13\cdot 19\cdot 67$.

⁵⁹Nouv. Ann. Math., (3), 3, 1884, 538-9.

⁶⁰Oeuvres, 2, 434, letter to Carcavi, Aug., 1659.

⁶¹Nouv. Ann. Math., (3), 2, 1883, 306-10. Cf. Chapter on Diophantine Equations of order 2.

⁶²L'intermédiaire des math., 7, 1900, 31, 84.

⁶³Nouv. Ann. Math., (2), 14, 1875, 335.

⁶⁴*Ibid.*, 509.

⁶⁵*Ibid.*, (2), 20, 1881, 150.

⁶⁶L'intermédiaire des math., 8, 1901, 149-150.

⁶⁷*Ibid.*, 22, 1915, 111-4, 127.

Gérardin⁶⁸ gave five new solutions of (i):

$$x = 3.11.31.443.499, \quad y = 2^9.3.5^4.13.37.61.157.$$

$$x = 2.3^3.31.443.449, \quad y = 2^7.3.5^4.11.13.37.61.157.$$

$$x = 11.17.41.43.239.307.443.499, \quad y = 2^{12}.3^3.5^7.7.11.13^3.29^2.37.61.157.$$

$$x = 2.11.17.23.41.211.467.577.853, \quad y = 2^{10}.3^4.5^3.7.13^2.17.29^2.53.61.113.193.197.$$

$$x = 3^3.11.13.23.83.193.701, \quad y = 2^9.3^3.5^3.7.11.13.17.53.61.97.149,$$

the last following from his⁶⁷ fourth pair in view of

$$\sigma(3^9.11^3): \sigma(2^3.3^3) = 2^5.3.11^2.61^2: 2^3.3.5^2 = 2^2.11^2.61^2: 5^2.$$

A. Cunningham and J. Blaikie⁶⁹ found solutions of the form $x = 2^r p$ of $s(x) = g^2$, where $s(n)$ is the sum of the divisors $< n$ of n .

PRODUCT OF ALIQUOT PARTS.

Paul Halcke⁷⁵ noted that the product of the aliquot parts of 12, 20, or 45 is the square of the number; the product for 24 or 40 is the cube; the product for 48, 80 or 405 is the biquadrate.

E. Lionnet⁷⁶ defined a perfect number of the second kind to be a number equal to the product of its aliquot parts. The only ones are p^3 and pq , where p and q are distinct primes.

⁶⁸L'intermédiaire des math., 24, 1917, 132-3.

⁶⁹Math. Quest. Educ. Times, (2), 7, 1905, 68-9.

⁷⁵Deliciae Math. oder Math. Sinnen-Confect, Hamburg, 1719, 197, Exs. 150-2.

⁷⁶Nouv. Ann. Math., (2), 18, 1879, 306-8. Lucas, Théorie des nombres, 1891, 373, Ex. 6

CHAPTER III.

FERMAT'S AND WILSON'S THEOREMS, GENERALIZATIONS AND CONVERSES; SYMMETRIC FUNCTIONS OF 1, 2, . . . , $P-1$ MODULO P .

FERMAT'S AND WILSON'S THEOREMS; IMMEDIATE GENERALIZATIONS.

The Chinese¹ seem to have known as early as 500 B. C. that 2^p-2 is divisible by the prime p . This fact was rediscovered by P. de Fermat² while investigating perfect numbers. Shortly afterwards, Fermat³ stated that he had a proof of the more general fact now known as Fermat's theorem: If p is any prime and x is any integer not divisible by p , then $x^{p-1}-1$ is divisible by p .

G. W. Leibniz⁴ (1646-1716) left a manuscript giving a proof of Fermat's theorem. Let p be a prime and set $x=a+b+c+\dots$. Then each multinomial coefficient appearing in the expansion of $x^p-\Sigma a^p$ is divisible by p . Take $a=b=c=\dots=1$. Thus x^p-x is divisible by p for every integer x .

G. Vacca⁵ called attention to this proof by Leibniz.

Vacca⁶ cited manuscripts of Leibniz in the Hannover Library showing that he proved Fermat's theorem before 1683 and that he knew the theorem now known as Wilson's¹⁷ theorem: If p is a prime, $1+(p-1)!$ is divisible by p . But Vacca did not explain an apparent obscurity in Leibniz's statement [cf. Mahnke⁷].

D. Mahnke⁷ gave an extensive account of those results in the manuscripts of Leibniz in the Hannover Library which relate to Fermat's and Wilson's theorems. As early as January 1676 (p. 41) Leibniz concluded, from the expressions for the y th triangular and y th pyramidal numbers, that

$$(y+1)y \equiv y^2 - y \equiv 0 \pmod{2}, \quad (y+2)(y+1)y \equiv y^3 - y \equiv 0 \pmod{3},$$

and similarly for moduli 5 and 7, whereas the corresponding formula for modulus 9 fails for $y=2$,—thus forestalling the general formula by Lagrange.¹⁸ On September 12, 1680 (p. 49), Leibniz gave the formula now known as Newton's formula for the sum of like powers and noted (by incomplete induction) that all the coefficients except the first are divisible by the exponent p , when p is a prime, so that

$$a^p + b^p + c^p + \dots \equiv (a+b+c+\dots)^p \pmod{p}.$$

Taking $a=b=\dots=1$, we obtain Fermat's theorem as above.⁴ That the binomial coefficients in $(1+1)^p-1-1$ are divisible by the prime p was

¹G. Peano, *Formulaire math.*, 3, Turin, 1901, p. 96. Jeans.²²⁰

²Oeuvres de Fermat, Paris, 2, 1894, p. 198, 2^o, letter to Mersenne, June (?), 1640; also p. 203, 2; p. 209.

³Oeuvres, 2, 209, letter to Frenicle de Bessy, Oct. 18, 1640; Opera Math., Tolosae, 1679, 163.

⁴Leibnizens Math. Schriften, herausgegeben von G. J. Gerhardt, VII, 1863, 180-1, "nova algebrae promotio."

⁵Bibliotheca math., (2), 8, 1894, 46-8.

⁶Bolletino di Bibliografia Storia Sc. Mat., 2, 1899, 113-6.

⁷Bibliotheca math., (3), 13, 1912-3, 29-61.

proved in 1681 (p. 50). Mahnke gave reasons (pp. 54-7) for believing that Leibniz rediscovered independently Fermat's theorem before he became acquainted, about 1681-2, with Fermat's *Varia opera math.* of 1679. In 1682 (p. 42), Leibniz stated that $(p-2)! \equiv 1 \pmod{p}$ if p is a prime [equivalent to Wilson's theorem], but that $(p-2)! \equiv m \pmod{p}$, if p is composite, m having a factor > 1 in common with p .

De la Hire⁸ stated that if k^{2r+1} is divided by $2(2r+1)$ we get k as a remainder, perhaps after adding a multiple of the divisor. For example, if k^5 is divided by 10 we get the remainder k . He remarked that Carré had observed that the cube of any number $k < 6$ has the remainder k when divided by 6.

L. Euler⁹ stated Fermat's theorem in the form: If $n+1$ is a prime dividing neither a nor b , then $a^n - b^n$ is divisible by $n+1$. He was not able to give a proof at that time. He stated the generalization: If $e = p^{m-1}(p-1)$ and if p is a prime, the remainder obtained on dividing a^e by p^m is 0 or 1 [a special case of Euler¹⁴]. He stated also that if m, n, p, \dots are distinct primes not dividing a and if A is the l. c. m. of $m-1, n-1, p-1, \dots$, then $a^A - 1$ is divisible by $mnp \dots$ [and $a^k - 1$ by $m^r n^s \dots$ if $k = A m^{r-1} n^{s-1} \dots$].

Euler¹⁰ first published a proof of Fermat's theorem. For a prime p ,

$$2^p = (1+1)^p = 1 + p + \binom{p}{2} + \dots + p + 1 = 2 + mp,$$

$$3^p = (1+2)^p = 1 + kp + 2^p, \quad 3^p - 3 - (2^p - 2) = kp,$$

$$(1+a)^p = 1 + np + a^p, \quad (1+a)^p - (1+a) - (a^p - a) = np.$$

Hence if $a^p - a$ is divisible by p , also $(1+a)^p - (1+a)$ is, and hence also $(a+2)^p - (a+2), \dots, (a+b)^p - (a+b)$. For $a=2$, $2^p - 2$ was proved divisible by p . Hence, writing x for $2+b$, we conclude that $x^p - x$ is divisible by p for any integer x .

G. W. Kraft¹¹ proved similarly that $2^p - 2 = mp$.

L. Euler's¹² second proof is based, like his first, on the binomial theorem. If a, b are integers and p is a prime, $(a+b)^p - a^p - b^p$ is divisible by p . Then, if $a^p - a$ and $b^p - b$ are divisible by p , also $(a+b)^p - a - b$ is divisible by p . Take $b=1$. Thus $(a+1)^p - a - 1$ is divisible by p if $a^p - a$ is. Taking $a=1, 2, 3, \dots$ in turn, we conclude that $2^p - 2, 3^p - 3, \dots, c^p - c$ are divisible by p .

L. Euler¹³ preferred his third proof to his earlier proofs since it avoids the use of the binomial theorem. If p is a prime and a is any integer not

⁸Hist. Acad. Sc. Paris, année 1704, pp. 42-4; mém., 358-362.

⁹Comm. Ac. Petrop., 6, 1732-3, 106; Comm. Arith., 1, 1849, p. 2. [Opera postuma, I, 1862, 167-8 (about 1778)].

¹⁰Comm. Ac. Petrop., 8, ad annum 1736, p. 141; Comm. Arith., 1, p. 21.

¹¹Novi Comm. Ac. Petrop., 3, ad annos 1750-1, 121-2.

¹²Novi Comm. Ac. Petrop., 1, 1747-8, 20; Comm. Arith., 1, 50. Also, letter to Goldbach, Mar. 6, 1742, Corresp. Math. Phys. (ed. Fuss), I, 1843, 117. An extract of the letter is given in Nouv. Ann. Math., 12, 1853, 47.

¹³Novi Comm. Ac. Petrop., 7, 1758-9, p. 70 (ed. 1761, p. 49); 18, 1773, p. 85; Comm. Arith., 1, 260-9, 518-9. Reproduced by Gauss, Disq. Arith., art. 49; Werke, 1, 1863, p. 40.

divisible by p , at most $p-1$ of the positive residues $< p$, obtained by dividing $1, a, a^2, \dots$ by p , are distinct. Let, therefore, a^μ and a^ν , where $\mu > \nu$, have the same residue. Then $a^{\mu-\nu} - 1$ is divisible by p . Let λ be the least positive integer for which $a^\lambda - 1$ is divisible by p . Then $1, a, a^2, \dots, a^{\lambda-1}$ have distinct residues when divided by p , so that $\lambda \leq p-1$. If $\lambda = p-1$, Fermat's theorem is proved. If $\lambda < p-1$, there exists a positive integer k ($k < p$) which is not the residue of a power of a . Then $k, ak, a^2k, \dots, a^{\lambda-1}k$ have distinct residues, no one the residue of a power of a . Since the two sets give 2λ distinct residues, we have $2\lambda \leq p-1$. If $\lambda < (p-1)/2$, we start with a new residue s and see that $s, as, a^2s, \dots, a^{\lambda-1}s$ have distinct residues, no one the residue of a power of a or of a^k . Hence $\lambda \leq (p-1)/3$. Proceeding in this manner, we see that λ divides $p-1$. Thus $a^{p-1} - 1$ is divisible by $a^\lambda - 1$ and hence by p .

L. Euler¹⁴ soon gave his fundamental generalization of Fermat's theorem from the case of a prime to any integer N :

Euler's theorem: If $n = \phi(N)$ is the number of positive integers not exceeding N and relatively prime to N , then $x^n - 1$ is divisible by N for every integer x relatively prime to N .

Let v be the least positive integer for which x^v has the residue 1 when divided by N . Then the residues of $1, x, x^2, \dots, x^{v-1}$ are distinct and prime to N . Thus $v \leq n$. If $v < n$, there is an additional positive integer a less than N and prime to N . Then, when $a, ax, ax^2, \dots, ax^{v-1}$ are divided by N , the residues are distinct from each other and from those of the powers of x . Thus, $2v \leq n$. Similarly, if $2v < n$, then $3v \leq n$. It follows in this manner that v divides n .

J. H. Lambert¹⁵ gave a proof of Fermat's theorem differing slightly from the first proof by Euler.¹⁰ If b is not divisible by the prime p , $b^{p-1} - 1$ is divisible by p . For, set $b = c + 1$. Then

$$\begin{aligned} b^{p-1} - 1 &= -1 + c^{p-1} + (p-1)c^{p-2} + \dots + 1 \\ &= -1 + c^{p-1} - c^{p-2} + c^{p-3} - \dots + 1 + Ap, \end{aligned}$$

where A is an integer. The intermediate terms equal

$$\frac{c^p + 1}{c + 1} = c^{p-1} - \frac{c^{p-1} - 1}{c + 1}.$$

Hence

$$\frac{b^{p-1} - 1}{p} = \frac{c^{p-1} - 1}{p} + A - f, \quad f = \frac{c^{p-1} - 1}{p(c + 1)}.$$

The theorem will thus follow by induction if f is shown to be integral. [Take $p > 2$, so that $p-1$ is even.] Then $c^{p-1} - 1$ is divisible by $c + 1$, and by the hypothesis for the induction, by p . Since $c + 1 = b$ is relatively prime to p , f is an integer.

¹⁴Novi Comm. Ac. Petrop., 8, 1760-1, p. 74; Comm. Arith., 1, 274-286; 2, 524-6.

¹⁵Nova Acta Eruditorum, Lipsiae, 1769, 109.

E. Waring¹⁶ first published the theorem that [Leibniz⁶] $1+(p-1)!$ is divisible by the prime p , ascribing it to Sir John Wilson¹⁷ (1741-1793). Waring (p. 207; ed. 3, p. 356) proved that if $a^p - a$ is divisible by p , then $(a+1)^p - a - 1$ is, since $(a+1)^p = a^p + pA + 1$, "a property first invented by Dom. Beaufort and first proved by Euler."

J. L. Lagrange¹⁸ was the first to publish a proof of Wilson's theorem. Let

$$(x+1)(x+2)\dots(x+p-1) = x^{p-1} + A_1x^{p-2} + \dots + A_{p-1}.$$

Replace x by $x+1$ and multiply the resulting equation by $x+1$. Comparing with the original equation multiplied by $x+p$, we get

$$(x+p)(x^{p-1} + \dots + A_{p-1}) = (x+1)^p + A_1(x+1)^{p-1} + \dots + A_{p-1}(x+1).$$

Apply the binomial theorem and equate coefficients of like powers of x . Thus

$$A_1 = \binom{p}{2}, 2A_2 = \binom{p}{3} + \binom{p-1}{2}A_1, 3A_3 = \binom{p}{4} + \binom{p-1}{3}A_1 + \binom{p-2}{2}A_2, \dots$$

Let p be a prime. Then, for $0 < k < p$, $\binom{p}{k}$ is an integer divisible by p . Hence $A_1, 2A_2, \dots, (p-2)A_{p-2}$ are divisible by p . Also,

$$(p-1)A_{p-1} = \binom{p}{p} + \binom{p-1}{p-1}A_1 + \binom{p-2}{p-2}A_2 + \dots = 1 + A_1 + A_2 + \dots + A_{p-2}.$$

Thus $1 + A_{p-1}$ is divisible by p . By the original equation, $A_{p-1} = (p-1)!$, so that Wilson's theorem follows.

Moreover, if x is any integer, the proof shows that

$$x^{p-1} - 1 - (x+1)(x+2)\dots(x+p-1)$$

is divisible by the prime p . If x is not divisible by p , some one of the integers $x+1, \dots, x+p-1$ is divisible by p . Hence $x^{p-1} - 1$ is divisible by p , giving Fermat's theorem.

Lagrange deduced Wilson's theorem from Fermat's. By the formula¹⁹ for the differences of order $p-1$ of $1^{p-1}, \dots, n^{p-1}$,

$$(1) \quad (p-1)! = p^{p-1} - (p-1)(p-1)^{p-1} + \binom{p-1}{2}(p-2)^{p-1} \\ - \binom{p-1}{3}(p-3)^{p-1} + \dots + (-1)^{p-1}.$$

Dividing the second member by p , and applying Fermat's theorem, we obtain the residue

$$-(p-1) + \binom{p-1}{2} - \binom{p-1}{3} + \dots + (-1)^{p-1} = (1-1)^{p-1} - 1 = -1.$$

¹⁶Meditationes algebraicae, Cambridge, 1770, 218; ed. 3, 1782, 380.

¹⁷On his biography see Nouv. Corresp. Math., 2, 1876, 110-114; M. Cantor, Bibliotheca math., (3), 3, 1902, 412; 4, 1903, 91.

¹⁸Nouv. Mém. Acad. Roy. Berlin, 2, 1773, année 1771, p. 125; Oeuvres, 3, 1869, 425. Cf. N. Nielsen, Danske Vidensk. Selsk. Forh., 1915, 520.

¹⁹Euler, Novi Comm. Ac. Petrop., 5, 1754-5, p. 6; Comm. Arith., 1, p. 213; 2, p. 532; Opera postuma, Petropoli, 1, 1862, p. 32.

Finally, Lagrange proved the converse of Wilson's theorem: If n divides $1 + (n-1)!$, then n is a prime. For $n = 4m+1$, n is a prime if $(2 \cdot 3 \dots 2m)^2$ has the remainder -1 when divided by n . For $n = 4m-1$, if $(2m-1)!$ has the remainder ± 1 .

L. Euler²⁰ also proved by induction from $x = n$ to $n+1$ that

$$(2) \quad x! = a^x - x(a-1)^x + \binom{x}{2}(a-2)^x - \binom{x}{3}(a-3)^x + \dots,$$

which reduces to (1) for $x = p-1$, $a = p$; and more generally,

$$(3) \quad a^x - n(a-1)^x + \binom{n}{2}(a-2)^x - \dots + (-1)^k \binom{n}{k}(a-k)^x + \dots = \begin{cases} 0 & \text{if } x < n \\ n! & \text{if } x = n. \end{cases}$$

D'Alembert²¹ stated that the theorem that the difference of order m of a^m is $m!$ had been long known and gave a proof.

L. Euler²² made use of a primitive root a of the prime p to prove Wilson's theorem (though his proof of the existence of a was defective). When $1, a, a^2, \dots, a^{p-2}$ are divided by p , the remainders are $1, 2, 3, \dots, p-1$ in some order. Hence $a^{(p-1)(p-2)/2}$ has the same remainder as $(p-1)!$. Taking $p > 2$, we may set $p = 2n+1$. Since a^n has the remainder -1 , then $a^n a^{2n(n-1)}$, and hence also $(p-1)!$, has the remainder -1 .

P. S. Laplace²³ proved Fermat's theorem essentially by the first method of Euler¹⁰ without citing him: If a is an integer $< p$ not divisible by the prime p ,

$$\frac{a^p}{a} = \frac{1}{a}(a-1+1)^p = \frac{1}{a}\{(a-1)^p + p(a-1)^{p-1} + \dots + 1\},$$

$$a^{p-1} - 1 = \frac{1}{a}\{(a-1)^p + 1 - a + hp(a-1)\} = \frac{a-1}{a}\{(a-1)^{p-1} - 1 + hp\}.$$

Hence by induction $a^{p-1} - 1$ is divisible by p . For $a > p$, set $a = np + q$ and use the theorem for q .

He gave a proof of Euler's¹⁴ generalization by the method of powering: if $n = p^\mu p_1^{\mu_1} \dots$, where p, p_1, \dots are distinct primes, and if a is prime to n , then $a^n - 1$ is divisible by n , where

$$v = n \left(\frac{p-1}{p} \right) \left(\frac{p_1-1}{p_1} \right) \dots = qr,$$

$$q = p^{\mu-1}(p-1), \quad r = p_1^{\mu_1-1}(p_1-1)p_2^{\mu_2-1}(p_2-1) \dots$$

Set $a^q = x$. Then $a^v - 1 = x^r - 1$ is divisible by $x-1$. Using the binomial theorem and $a^{p-1} - 1 = hp$, we find that $x-1$ is divisible by p^μ .

²⁰Novi Comm. Ac. Petrop., 13, 1768, 28-30.

²¹Letter to Turgot, Nov. 11, 1772, in unedited papers in the Bibliothèque de l'Institut de France. Cf. Bull. Bibl. Storia Sc. Mat. e Fis., 18, 1885, 531.

²²Opuscula analytica, St. Petersburg, 1, 1783 [Nov. 15, 1773], p. 329; Comm. Arith., 2, p. 44; letter to Lagrange (Oeuvres, 14, p. 235), Sept. 24, 1773; Euler's Opera postuma, I, 583.

²³De la Place, Théorie abrégée des nombres premiers, 1776, 16-23. His proofs of Fermat's and Wilson's theorems were inserted at the end of Bossut's Algèbre, ed. 1776, and reproduced by S. F. Lacroix, Traité du Calcul Diff. Int., Paris, ed. 2, vol. 3, 1818, 722-4, on p. 10 of which is a proof of (2) for $a = x$ by the calculus of differences.

From the $(p-1)$ th order of differences for $x^{p-1}-1$,

$$(x+p-1)^{p-1}-1-(p-1)\{(x+p-2)^{p-1}-1\}+\binom{p-1}{2}\{(x+p-3)^{p-1}-1\} \\ -\dots+x^{p-1}-1=(p-1)!.$$

Set $x=1$ and use Fermat's theorem. Hence $1+(p-1)!$ is divisible by p .
E. Waring,¹⁶ 1782, 380-2, made use of

$$x^r = x(x-1)\dots(x-r+1) + Px(x-1)\dots(x-r+2) \\ + Qx(x-1)\dots(x-r+3) + \dots + Hx(x-1) + Ix,$$

where $P=1+2+\dots+(r-1)$, $Q=PA^1-B$, etc., B denoting the sum of the products of $1, 2, \dots, r-1$ two at a time, and $A^1=1+2+\dots+(r-2)$. Then

$$1^r+2^r+\dots+x^r = \frac{1}{r+1}(x+1)x(x-1)\dots(x-r+1) + \frac{P}{r}(x+1)x\dots(x-r+2) \\ + \frac{Q}{r-1}(x+1)x\dots(x-r+3) + \dots + \frac{H}{3}(x+1)x(x-1) + \frac{I}{2}(x+1)x.$$

Take $r=x$ and let $x+1$ be a prime. By Fermat's theorem, $1^x, 2^x, \dots, x^x$ each has the remainder unity when divided by $x+1$, so that their sum has the remainder x . Thus $1+x!$ is divisible by $x+1$.

Genty²⁴ proved the converse of Wilson's theorem and noted that an equivalent test for the primality of p is that p divide $(p-n)!(n-1)!-(-1)^n$. For $n=(p+1)/2$, the latter expression is $\{(\frac{p-1}{2})!\}^2 \pm 1$ [Lagrange¹⁸].

Franz von Schaffgotsch²⁵ was led by induction to the fact (of which he gave no proof) that, if n is a prime, the numbers $2, 3, \dots, n-2$ can be paired so that the product of the two in any pair is of the form $xn+1$ and the two of a pair are distinct. Hence, by multiplication, $2 \cdot 3 \dots (n-2)$ has the remainder unity when divided by n , so that $(n-1)!$ has the remainder $n-1$. For example, if $n=19$, the pairs are $2 \cdot 10, 4 \cdot 5, 3 \cdot 13, 7 \cdot 11, 6 \cdot 16, 8 \cdot 12, 9 \cdot 17, 14 \cdot 15$. Similarly, for n any power of a prime p , we can so pair the integers $< n-1$ which are not divisible by p . But for $n=15$, 4 and 4 are paired, also 11 and 11. Euler²⁶ had already used these associated residues (*residua sociata*).

F. T. Schubert^{26a} proved by induction that the n th order of differences of $1^n, 2^n, \dots$ is $n!$.

A. M. Legendre²⁷ reproduced the second proof by Euler¹² of Fermat's theorem and used the theory of differences to prove (2) for $a=x$. Taking $x=p-1$ and using Fermat's theorem, we get $(p-1)! \equiv (1-1)^p-1 \pmod{p}$.

²⁴Histoire et mém. de l'acad. roy. sc. insc. de Toulouse, 3, 1788 (read Dec. 4, 1783), p. 91.

²⁵Abhandlungen d. Böhmischen Gesell. Wiss., Prag, 2, 1786, 134.

²⁶Opusc. anal., 1, 1783 (1772), 64, 121; Novi Comm. Ac. Petrop., 18, 1773, 85, §26; Comm. Arith. 1, 480, 494, 519.

^{26a}Nova Acta Acad. Petrop., 11, ad annum 1793, 1798, mem., 174-7.

²⁷Théorie des nombres, 1798, 181-2; ed. 2, 1808, 166-7.

C. F. Gauss²⁸ proved that, if n is a prime, $2, 3, \dots, n-2$ can be associated in pairs such that the product of the two of a pair is of the form $xn+1$. This step completes Schaffgotsch's²⁵ proof of Wilson's theorem.

Gauss²⁹ proved Fermat's theorem by the method now known to be that used by Leibniz⁴ and mentioned the fact that the reputed proof by Leibniz had not then been published.

Gauss³⁰ proved that if a belongs to the exponent t modulo p , a prime, then $a \cdot a^2 \cdot a^3 \dots a^t \equiv (-1)^{t+1} \pmod{p}$. In fact, a primitive root ρ of p may be chosen so that $a \equiv \rho^{(p-1)/t}$. Thus the above product is congruent to ρ^k , where

$$k = (1+2+\dots+t) \left(\frac{p-1}{t} \right) = \frac{(t+1)(p-1)}{2}.$$

Thus $\rho^k = \left(\rho^{\frac{p-1}{2}} \right)^{t+1} \equiv (-1)^{t+1} \pmod{p}$. When a is a primitive root, a, a^2, \dots, a^{p-1} are congruent to $1, 2, \dots, p-1$ in some order. Hence $(p-1)! \equiv (-1)^p$. This method of proving Wilson's theorem is essentially that of Euler.²²

Gauss³¹ stated the generalization of Wilson's theorem: The product of the positive integers $< A$ and prime to A is congruent modulo A to -1 if $A=4, p^m$ or $2p^m$, where p is an odd prime, but to $+1$ if A is not of one of these three forms. He remarked that a proof could be made by use of associated numbers²⁸ with the difference that $x^2 \equiv 1 \pmod{A}$ may now have roots other than ± 1 ; also by use of indices and primitive roots³⁰ of a composite modulus.

S. F. Lacroix³² reproduced Euler's¹³ third proof of Fermat's theorem without giving a reference.

James Ivory³³ obtained Fermat's theorem by a proof later rediscovered by Dirichlet.⁴⁰ Let N be any integer not divisible by the prime p . When the multiples $N, 2N, 3N, \dots, (p-1)N$ are divided by p , there result p distinct positive remainders $< p$, so that these remainders are $1, 2, \dots, p-1$ in some order.³⁴ By multiplication, $N^{p-1}Q = Q + mp$, where $Q = (p-1)!$. Hence p divides $N^{p-1} - 1$ since it does not divide Q .

Gauss³⁵ used the last method in his proof of the lemma (employed in his third proof of the quadratic reciprocity law): If k is not divisible by the odd prime p , and if exactly μ of the least positive residues of $k, 2k, \dots, \frac{1}{2}(p-1)k$ modulo p exceed $p/2$, then $k^{(p-1)/2} \equiv (-1)^\mu \pmod{p}$. [Cf. Grunert.⁴⁵]

²⁸Disquisitiones Arith., 1801, arts. 24, 77; Werke, 1, 1863, 19, 61.

²⁹Disq. Arith., art. 51, footnote to art. 50.

³⁰Disq. Arith., art. 75.

³¹Disq. Arith., art. 78.

³²Complément des élémens d'algèbre, Paris, ed. 3, 1804, 298-303; ed. 4, 1817, 313-7.

³³New Series of the Math. Repository (ed. Th. Leybourn), vol. 1, pt. 2, 1806, 6-8.

³⁴A fact known to Euler, Novi Comm. Acad. Petrop., 8, 1760-1, 75; Comm. Arith., 1, 275; and to Gauss, Disq. Arith., art. 23. Cf. G. Tarry, Nouv. Ann. Math., 18, 1899, 149, 292.

³⁵Comm. soc. reg. sc. Gottingensis, 16, 1808; Werke, 2, 1-8. Gauss' Höhere Arith., German transl. by H. Maser, Berlin, 1889, p. 458.

J. A. Grunert³⁶ considered the series

$$[m, n] = n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \dots,$$

to which Euler's (3) reduces for $a = n$, $x = m$, and proved that

$$[m, n] = n \{ [m-1, n-1] + [m-1, n] \}.$$

This recursion formula gives

$$\begin{aligned} [m, n] &= 0 \quad (m=0, 1, \dots, n-1); & [n, n] &= n! \text{ [cf. (2)]}, \\ [n+1, n] &= n! \binom{n+1}{2}, & [n+2, n] &= n! \binom{n+2}{3} \cdot \frac{3n+1}{4}, \\ [n+3, n] &= n! \binom{n+1}{2} \binom{n+3}{4}. \end{aligned}$$

Any $[m, n]$ is divisible by $n!$. As by the proof of Lagrange,¹⁸ $[m, n] + (-1)^n$ is divisible by $m+1$ if the latter is a prime $> n$. Again,

$$m!h^m = (x+mh)^m - m \{ x + (m-1)h \}^m + \binom{m}{2} \{ x + (m-2)h \}^m + \dots + (-1)^m x^m,$$

which for $x=0$, $h=1$, gives $[m, m] = m!$.

W. G. Horner³⁷ proved Euler's theorem by generalizing Ivory's³³ method. If r_1, \dots, r_φ are the integers $< m$ and prime to m , then $r_1N, \dots, r_\varphi N$ have the r 's as their residues modulo m .

P. F. Verhulst³⁸ gave Euler's proof²² in a slightly different form.

F. T. Poselger³⁹ gave essentially Euler's¹⁰ first proof.

G. L. Dirichlet⁴⁰ derived Fermat's and Wilson's theorems from a common source. Call m and n corresponding numbers if each is less than the prime p and if $mn \equiv a \pmod{p}$, where a is a fixed integer not divisible by p (thus generalizing Euler's²⁶ associated numbers). Each number $1, 2, \dots, p-1$ has one and but one corresponding number. If $x^2 \equiv a \pmod{p}$ has no integral solution, corresponding numbers are distinct and

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

But if k is a positive integer $< p$ such that $k^2 \equiv a \pmod{p}$, the second root is $p-k$, and the product of the numbers $1, \dots, p-1$, other than k and $p-k$, has the same residue as $a^{(p-3)/2}$, whence

$$(p-1)! \equiv -a^{(p-1)/2} \pmod{p}.$$

The case $a=1$ leads to Wilson's theorem. By the latter, we have

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p},$$

³⁶Math. Abhandlungen, Erste Sammlung, Altona, 1822, 67-93. Some of the results were quoted by Grunert, Archiv Math. Phys., 32, 1859, 115-8. For an interpretation in factoring of $[m, n]$, see Minetola¹⁶⁶ of Ch. X.

³⁷Annals of Phil. (Mag. Chem. . . .), new series, 11, 1826, 81.

³⁸Corresp. Math. Phys. (ed. Quételet), 3, 1827, 71.

³⁹Abhand. Ak. Wiss. Berlin (Math.), 1827, 21.

⁴⁰Jour. für Math., 3, 1828, 390; Werke, 1, 1889, 105. Dirichlet,⁶⁶ §34.

the sign being $+$ or $-$ according as $k^2 \equiv a \pmod{p}$ has or has not integral solutions (Euler's criterion). Squaring, we obtain Fermat's theorem. Finally, Dirichlet rediscovered the proof by Ivory.³³ [Cf. Moreau.¹²³]

J. Binet⁴¹ also rediscovered the proof by Ivory.³³

A. Cauchy⁴² gave a proof analogous to that by Euler.¹⁰

An anonymous writer⁴³ proved that if n is a prime the binomial coefficient $(n-1)_k$ has the residue $(-1)^k$ modulo n , so that

$$(1+x)^{n-1} - 1 \equiv -x + x^2 - \dots + x^{n-1}, \quad (1+x) \{ (1+x)^{n-1} - 1 \} \equiv x(x^{n-1} - 1),$$

modulo n . Thus Fermat's theorem follows by induction on x as in the proof by Euler.¹²

V. Bouniakowsky⁴⁴ gave a proof of Euler's theorem similar to that by Laplace.²³ If $a \equiv b$ is divisible by a prime p , $a^{p^{n-1} \pm b^{p^{n-1}}}$ is divisible by p^n , provided $p > 2$ when the sign is plus. Hence if p, p', \dots are distinct primes, $a^t \equiv b^t$ is divisible by $N = p^n p'^{n'} \dots$, where $t = p^{n-1} p'^{n'-1} \dots$, if $a \equiv b$ is divisible by $pp' \dots$, provided the p 's are > 2 if the sign is plus. Replace a by its $(p-1)$ th power and b by 1 and use Fermat's theorem; we see that $a^e - 1$ is divisible by N if $e = \phi(N)$. The same result gives a generalization of Wilson's theorem⁶

$$\{(p-1)!\}^{p^{n-1}} + 1 \equiv 0 \pmod{p^n}.$$

He gave (*ibid.*, 563-4) Gauss'³⁰ proof of Wilson's theorem.

J. A. Grunert⁴⁵ used the known fact that, if $0 < k < p$, then $k, 2k, \dots, (p-1)k$ are congruent to $1, 2, \dots, p-1$ in some order modulo p , a prime, to show that $kx \equiv 1 \pmod{p}$ has a unique root x . Wilson's theorem then follows as by Gauss. If (*ibid.*, p. 1095) we square Gauss' formula,³⁵ we get Fermat's theorem.

Giovanni de Paoli⁴⁶ proved Fermat's and Euler's theorems. In

$$(x+1)^p = x^p + 1 + pS_x,$$

where p is a prime, S_x is an integer. Change x to $x-1, \dots, 2, 1$ and add the resulting equations. Thus

$$x^p - x = p \sum_{z=1}^{x-1} S_z.$$

Replace x by x^m , divide by x^m and set $y = x^{p-1}$. Thus

$$y^m - 1 = pX_m, \quad X_m = \sum S_z^m / x^m = \text{integer}.$$

Replace m by $2m, \dots, (p-1)m$, add the resulting equations, and set $Y_m = 1 + X_m + X_{2m} + \dots + X_{(p-1)m}$. Thus

$$y^{mp} - 1 = p(y^m - 1)Y_m = p^2 X_m Y_m.$$

⁴¹Jour. de l'école polytechnique, 20, 1831, 291 (read 1827). Cauchy, Comptes Rendus Paris, 12, 1841, 813, ascribed the proof to Binet.

⁴²Exer. de math., 4, 1829, 221; Oeuvres, (2), 9, 263. Résumé analyt., Turin, 1, 1833, 10.

⁴³Jour. für Math., 6, 1830, 100-6.

⁴⁴Mém. Ac. Sc. St. Pétersbourg, Sc. Math. Phys. et Nat., (6), 1, 1831, 139 (read Apr. 1, 1829).

⁴⁵Klügel's Math. Wörterbuch, 5, 1831, 1076-9.

⁴⁶Opuscoli Matematici e Fisici di Diversi Autori, Milano, 1, 1832, 262-272.

a single term of a row is $\equiv 1 \pmod{p}$. If this term be $r_k a^2 r_k$, replace it by $(p-r_k) a^2 r_k \equiv -1$. Next, if $r_n a^2 r_k \equiv \mp 1$, $r_n a^2 r_i \equiv \pm 1$, then $r_k + r_i = p$ and one of the r_n is replaced by $p-r_n$. Hence we may separate $r_1 a, \dots, r_q a$ into $q/2$ pairs such that the product of the two of a pair is $\equiv \pm 1 \pmod{p}$. Taking $a=1$, we get $r_1 \dots r_q \equiv \pm 1 \pmod{p}$. The sign was determined only for the case p a prime (by Gauss' method).

A. Cauchy⁵⁰ derived Wilson's theorem from (1), page 62 above.

*Caraffa⁵¹ gave a proof of Fermat's theorem.

E. Midy⁵² gave Ivory's³³ proof of Fermat's theorem.

W. G. Horner⁵³ gave Euler's¹⁴ proof of his theorem.

G. Libri⁵⁴ reproduced Euler's proof¹² without a reference.

Sylvester⁵⁵ gave the generalized Wilson theorem in the incomplete form that the residue is ± 1 .

Th. Schönemann⁵⁶ proved by use of symmetric functions of the roots that if $z^n + b_1 z^{n-1} + \dots = 0$ is the equation for the p th powers of the roots of $x^n + a_1 x^{n-1} + \dots = 0$, where the a 's are integers and p is a prime, then $b_i \equiv a_i^p \pmod{p}$. If the latter equation is $(x-1)^n = 0$, the former is $z^n - (n^p + pQ)z^{n-1} + \dots = 0$, and yet is evidently $(z-1)^n = 0$. Hence $n^p \equiv n \pmod{p}$.

W. Brennecke⁵⁷ elaborated one of Gauss'³¹ suggestions for a proof of the generalized Wilson theorem. For $a > 2$, $x^2 \equiv 1 \pmod{2^a}$ has exactly four incongruent roots, $\pm 1, \pm(1+2^{a-1})$, since one of the factors $x \pm 1$, of difference 2, must be divisible by 2 and the other by 2^{a-1} . For p an odd prime, let r_1, \dots, r_μ be the positive integers $< p^a$ and prime to p^a , taking $r_1 = 1, r_\mu = p^a - 1$. For $2 \leq s \leq \mu - 1$, the root x of $r_s x \equiv 1 \pmod{p^a}$ is distinct from r_1, r_μ, r_s . Thus $r_2, \dots, r_{\mu-1}$ may be paired so that the product of the two of a pair is $\equiv 1 \pmod{p^a}$. Hence $r_1 \dots r_\mu \equiv -1 \pmod{p^a}$. This holds also for modulus $2p^a$. For $a > 2$,

$$(2^{a-1} - 1)(2^{a-1} + 1) \equiv -1, \quad r_1 \dots r_\mu \equiv +1 \pmod{2^a}.$$

Finally, let $N = p^a M$, where M is divisible by an odd prime, but not by p . Then $m = \phi(M)$ is even. The integers $< N$ and prime to p are

$$r_j, r_j + p^a, r_j + 2p^a, \dots, r_j + (M-1)p^a \quad (j=1, \dots, \mu).$$

For a fixed j , we obtain m integers $< N$ and prime to N . Hence if $\{N\}$ denotes the product of all the integers $< N$ and prime to N ,

$$\{N\} \equiv (r_1 \dots r_\mu)^m \equiv 1 \pmod{p^a}.$$

For $N = p^a q^\beta \dots$, $\{N\} \equiv 1 \pmod{q^\beta}, \dots$, whence $\{N\} \equiv 1 \pmod{N}$.

⁵⁰Résumé analyt., Turin, 1, 1833, 35.

⁵¹Elem. di mat. commentati da Volpicelli, Rome, 1836, I, 89.

⁵²De quelques propriétés des nombres, Nantes, 1836.

⁵³London and Edinb. Phil. Mag., 11, 1837, 456.

⁵⁴Mém. divers savants ac. sc. Institut de France (math.), 5, 1838, 19.

⁵⁵Phil. Mag., 13, 1838, 454 (14, 1839, 47); Coll. Math. Papers, 1, 1904, 39.

⁵⁶Jour. für Math., 19, 1839, 290; 31, 1846, 288. Cf. J. J. Sylvester, Phil. Mag., (4), 18, 1859, 281.

⁵⁷Jour. für Math., 19, 1839, 319.

A. L. Crelle⁵⁸ proved the generalized Wilson theorem. By pairing each root σ of $x^2 \equiv 1 \pmod{s}$ with the root $s - \sigma$, and each integer $a < s$, prime to s and not a root, with its associated number a' , where $aa' \equiv 1 \pmod{s}$, we see that the product of all the integers $< s$ and prime to s is $\equiv +1$ or $-1 \pmod{s}$ according as the number n of pairs of roots $\sigma, s - \sigma$ is even or odd. To find n , express s in every way as a product of two factors u, v , whose g. c. d. is 1 or 2; in the respective cases, each factor pair gives a single root σ or two roots. Treating four subcases at length it is shown that the number of factor pairs is 2^k in each case, where k is the number of distinct odd primes dividing s ; and then that n is odd if $s = 4, p^m$ or $2p^n$, but even if n is not of one of these three forms.

A. Cauchy^{58a} proved Fermat's theorem as had Leibniz.⁴

V⁵⁹ (S. Earnshaw?) proved Wilson's theorem by Lagrange's method and noted that, if S_r is the sum of the products of the roots of $A_0x^m + A_1x^{m-1} + \dots \equiv 0 \pmod{p}$ taken r at a time, then $A_0S_r - (-1)^r A_r$ is divisible by p .

Paolo Gorini⁶⁰ proved Euler's theorem $b^t \equiv 1 \pmod{\Delta}$, where $t = \phi(\Delta)$, by arranging in order of magnitude the integers (A) $p', p'', \dots, p^{(t)}$ which are less than Δ and prime to Δ . After omitting the numbers in (A) which are divisible by b , we obtain a set (B) $q', \dots, q^{(l)}$. Let $q^{(\omega)}$ be the least of the latter which when increased by Δ gives a multiple of b :

$$(C) \quad q^{(\omega)} + \Delta = p^{(a)}b.$$

The numbers* (A) coincide with those in sets (B) and (D):

$$(D) \quad p'b, p''b, \dots, p^{(a-1)}b.$$

Hence by multiplication and cancellation of $p', \dots, p^{(a-1)}$,

$$(F) \quad q' \dots q^{(l)} b^{a-1} = p^{(a)} \dots p^{(t)}.$$

To each number (B) add the least multiple of Δ which gives a sum divisible by b , say (G) $q' + g'\Delta, \dots, q^{(l)} + g^{(l)}\Delta$. The least of these is $q^{(\omega)} + \Delta = p^{(a)}b$, by (C). Each number (G) is $< b\Delta$ and all are distinct. The quotients obtained by dividing the numbers (G) by b are prime to Δ and hence included among the $p^{(a)}, \dots, p^{(t)}$, whose number is $t - a + 1 = l$, so that each arises as a quotient. Hence

$$(H) \quad \prod_{i=1}^l (q^{(i)} + g^{(i)}\Delta) = P\Delta + q' \dots q^{(l)} = p^{(a)} p^{(a+1)} \dots p^{(t)} b^{t-a+1}.$$

Combine this with (F) to eliminate the p 's. We get

$$q' \dots q^{(l)} b^{a-1} b^{t-a+1} = P\Delta + q' \dots q^{(l)}, \quad q' \dots q^{(l)} (b^t - 1) = P\Delta, \quad b^t - 1 = Q\Delta.$$

⁵⁸Jour. für Math., 20, 1840, 29-56. Abstract in Bericht Akad. Wiss. Berlin, 1839, 133-5.

^{58a}Mém. Ac. Sc. Paris, 17, 1840, 436; Oeuvres, (I), 3, 163-4.

⁵⁹Cambr. Math. Jour., 2, 1841, 79-81.

⁶⁰Annali di Fisica, Chimica e Mat. (ed., G. A. Majocchi), Milano, 1, 1841, 255-7.

*To follow the author's steps, take $\Delta = 15, b = 2$, whence $t = 8, l = 4$, (A) 1, 2, 4, 7, 8, 11, 13, 14; (B) 1, 7, 11, 13; (C) $1 + 15 = 8 \cdot 2, p^{(a)} = 8, a = 5$; (D) 2, 4, 8, 14; (F) $1 \cdot 7 \cdot 11 \cdot 13 \cdot 2^4 = 8 \cdot 11 \cdot 13 \cdot 14$; (G) $1 + 15, 7 + 15, 11 + 15, 13 + 15$, each $g = 1$; the quotients of the latter by 2 are 8, 11, 13, 14, viz., last four in (A); (H) $P \cdot 15 + 1 \cdot 7 \cdot 11 \cdot 13 = 8 \cdot 11 \cdot 13 \cdot 14 \cdot 2$; the second member is $1 \cdot 7 \cdot 11 \cdot 13 \cdot 2^8$ by (F). Hence $1 \cdot 7 \cdot 11 \cdot 13 (2^8 - 1) = 15P$.

E. Lionnet⁶¹ proved that, if p is an odd prime, the sum of the m th powers of $1, \dots, p-1$ is divisible by p for $0 < m < p-1$. Hence the sum P_m of the products of $1, \dots, p-1$ taken m at a time is divisible by p [Lagrange¹⁸]. Since

$$(1+1)(1+2)\dots(1+p-1) = 1 + P_1 + P_2 + \dots + P_{p-2} + (p-1)!,$$

$1 + (p-1)!$ is divisible by p .

E. Catalan⁶² gave the proofs by Ivory³³ and Horner.³⁷ C. F. Arndt⁶³ gave Horner's proof; and proved the generalized Wilson theorem by associated numbers. O. Terquem⁶⁴ gave the proofs by Gauss²³ and Dirichlet.⁴⁰

A. L. Crelle⁶⁵ republished his proof⁴⁷ of Wilson's theorem, as well as that by Gauss³⁰ and Dirichlet.⁴⁰ Crelle⁶⁶ gave two proofs of the generalized Wilson theorem, essentially that by Minding⁴⁸ and that given by himself.⁵⁸ If μ is the number of distinct odd prime factors of z , and 2^m is the highest power of 2 dividing z , and r is a quadratic residue of z , then (p. 150) the number n of pairs of roots $\pm x$ of $x^2 \equiv r \pmod{z}$ is $2^{\mu-1}$ if $m=0$ or 1, 2^μ if $m=2$, $2^{\mu+1}$ if $m>2$. Using the fact (p. 122) that the quadratic residues of z are the $e=\phi(z)/(2n)$ roots of $r^e \equiv 1 \pmod{z}$, it is shown (p. 173) that, if v is any integer prime to z , $v^{\phi(z)/n} \equiv 1 \pmod{z}$, "a perfection of the Euler-Fermat theorem."

L. Poinso⁶⁷ failed in his attempt to prove the generalized Wilson theorem. He began as had Crelle.⁵⁸ But he stated incorrectly that the number n of pairs of roots $\pm x$ of $x^2 \equiv 1 \pmod{s}$ equals the number v of ways of expressing s as a product of two factors P, Q whose g. c. d. is 1 or 2. For each pair $\pm x$, it is implied that $x-1$ and $x+1$ uniquely determine P, Q . For $s=24$, $n=v=4$; but for the root $x=7$ (or for $x=17$), $x \pm 1$ yield $P, Q=3, 8$, and $6, 4$. To correct another error by Poinso^t, let μ be the number of distinct odd prime factors of s and let 2^m be the highest power of 2 dividing s ; then $v=2^{\mu-1}, 2^\mu, 3 \cdot 2^{\mu-1}$ or $2^{\mu+1}$, according as $m=0, 1, 2$, or ≥ 3 , whereas [Crelle⁶⁶] $n=2^{\mu-1}, 2^{\mu-1}, 2^\mu, 2^{\mu+1}$. No difficulty is met (pp. 53-5) in case the modulus is a power of a prime. He noted (p. 33) that if r_1, r_2, \dots are the integers $< N$ and prime to N , and π is their product, they are congruent modulo N to $\pi/r_1, \pi/r_2, \dots$, whence $\pi \equiv \pi^{\nu-1} \pmod{N}$, where $\nu=\phi(N)$. Thus, by Euler's theorem, $\pi^2 \equiv 1$. This does not imply that $\pi \equiv \pm 1$ as cited by Aubry,¹³⁷ pp. 300-1.

Poinso^t (p. 51) proved Euler's theorem by considering a regular polygon of N sides. Let x be prime to N and $< N$. Join any vertex with the x th vertex following it, the new vertex with the x th vertex following it, etc., thus defining a regular (star) polygon of N sides. With the same x , derive

⁶¹Nouv. Ann. Math., 1, 1842, 175-6.

⁶²Ibid., 462-4.

⁶³Archiv Math. Phys., 2, 1842, 7, 22, 23.

⁶⁴Nouv. Ann. Math., 2, 1843, 193; 4, 1845, 379.

⁶⁵Jour. für Math., 28, 1844, 176-8.

⁶⁶Ibid., 29, 1845, 103-176.

⁶⁷Jour. de Math., 10, 1845, 25-30. German exposition by J. A. Grunert, Archiv Math. Phys., 7, 1846, 168, 367.

similarly a new N -gon, etc., until the initial polygon is reached.⁶⁸ The number μ of distinct polygons thus obtained is seen to be a divisor of $\phi(N)$, the number of polygons corresponding to the various x 's. If in the initial polygon we take the x^μ th vertex following any one, etc., we obtain the initial polygon. Hence x^μ and thus also $x^{\phi(N)}$ has the remainder unity when divided by N . [When completed this proof differs only slightly from that by Euler.¹⁴]

E. Prouhet⁶⁹ modified Poincot's method and obtained a correct proof of the generalized Wilson theorem. Let r be the number of roots of $x^2 \equiv 1 \pmod{N}$, and w the number of ways of expressing N as a product of two relatively prime factors. If $N = 2^m p_1^{\pi_1} \dots p_\mu^{\pi_\mu}$, where the p 's are distinct odd primes, evidently $w = 2^\mu$ if $m > 0$, $w = 2^{\mu-1}$ if $m = 0$. By considering divisors of $x \not\equiv 1$, it is proved that $r = 2w$ if $m = 0$ or 2 , $r = w$ if $m = 1$, $r = 4w$ if $m > 2$. Hence $r = 2^\mu$ if $m = 0$ or 1 , $2^{\mu+1}$ if $m = 2$, $2^{\mu+2}$ if $m > 2$. By Crelle,⁵⁸ the product P of the integers $< N$ and prime to N is $\equiv (-1)^{r/2} \pmod{N}$. Thus for $\mu > 0$, $P \equiv +1$ unless $m = 0$ or 1 , $\mu = 1$, viz., $N = p^\pi$ or $2p^\pi$; while, for $\mu = 0$, $N = 2^m$, $m > 2$, we have $r = 4$, $P \equiv +1$.

Friderico Arndt⁷⁰ elaborated Gauss³¹ second suggestion for a proof of the generalized Wilson theorem. Let g be a primitive root of the modulus p^n or $2p^n$, where p is an odd prime. Set $v = \phi(p^n)$. Then g, g^2, \dots, g^v are congruent to the numbers less than the modulus and prime to it. If P is the product of the latter, $P \equiv g^{v(v+1)/2}$. But $g^{v/2} \equiv -1$. Hence $P \equiv -1$. Next, if $n > 2$, the product of the incongruent numbers belonging to an exponent 2^{n-m} is $\equiv 1 \pmod{2^n}$. Next, consider the modulus $M = AB$, where A and B are relatively prime. The positive integers $< M$ and prime to M are congruent modulo M to $Ay_i + Bx_j$, where the x_i are $< A$ and prime to A , the y_j are $< B$ and prime to B . But, if $a = \phi(A)$,

$$\pi_1 = \prod_{j=1}^a (Ay_1 + Bx_j) \equiv B^a x_1 \dots x_a \equiv x_1 \dots x_a \pmod{A},$$

$$P = \pi_1 \pi_2 \dots \equiv (x_1 \dots x_a)^{\phi(B)} \pmod{A}.$$

By resolving M into a product of powers of primes and applying the above results, we determine the sign in $P \equiv \pm 1 \pmod{M}$.

J. A. Grunert⁷¹ proved that if a prime $n+1 > 2$ divides no one of the integers a_1, \dots, a_n , nor any of their differences, it divides $a_1 a_2 \dots a_n + 1$, and stated that this result is much more general than Wilson's theorem (the case $a_j = j$). But the generalization is only superficial since a_1, \dots, a_n are congruent modulo $n+1$ to $1, \dots, n$ in some order. His proof employed Fermat's theorem and certain complex equations involving products of differences of n numbers and sums of products of n numbers taken m at a time.

J. F. Heather⁷² gave without reference the first results of Grunert.³⁶

⁶⁸Cf. P. Bachmann, *Die Elemente der Zahlentheorie*, 1892, 19–23.

⁶⁹Nouv. Ann. Math., 4, 1845, 273–8.

⁷⁰Jour. für Math., 31, 1846, 329–332.

⁷¹Archiv Math. Phys., 10, 1847, 312.

⁷²The Mathematician, London, 2, 1847, 296.

A. Lista⁷³ gave Lagrange's proof of Wilson's theorem.

V. Bouniakowsky⁷⁴ gave Euler's²² proof.

P. L. Tchebychef⁷⁵ concluded from Fermat's theorem that

$$(x-1)(x-2)\dots(x-p+1)-x^{p-1}+1\equiv 0 \pmod{p}$$

is an identity if p is a prime. Hence if s_j is the sum of the products of $1, \dots, p-1$ taken j at a time, $s_j \equiv 0 \pmod{p}$ ($j < p-1$), $s_{p-1} \equiv -1 \pmod{p}$, the last being Wilson's theorem.

Sir F. Pollock⁷⁶ gave an incomplete statement and proof of the generalized Wilson theorem by use of associated numbers. Likewise futile was his attempt to extend Dirichlet's⁴⁰ method [not cited] of association into pairs with the product $\equiv a \pmod{m}$ to the case of a composite m .

E. Desmarest⁷⁷ gave Euler's¹³ proof of Fermat's theorem.

O. Schlömilch^{77a} considered the quotient

$$\{n^p - \binom{n}{1}(n-1)^p + \binom{n}{2}(n-2)^p - \dots\}/n!$$

J. J. Sylvester⁷⁸ took $x=1, 2, \dots, p-1$ in turn in

$$(x-1)(x-2)\dots(x-p+1) = x^{p-1} + A_1x^{p-2} + \dots + A_{p-1},$$

where p is a prime. Since $x^{p-1} \equiv 1 \pmod{p}$, there result $p-1$ congruences linear and homogeneous in $A_1, \dots, A_{p-2}, A_{p-1}+1$, the determinant of whose coefficients is the product of the differences of $1, 2, \dots, p-1$ and hence not divisible by p . Thus $A_1 \equiv 0, \dots, A_{p-1}+1 \equiv 0$, the last giving Wilson's theorem.

W. Brennecke⁷⁹ proved Euler's theorem by the methods of Horner³⁷ and Laplace,²³ noting that

$$(a^{p-1})^p \equiv 1 \pmod{p^2}, \quad (a^{p-1})^{p^2} \equiv 1 \pmod{p^3}, \dots$$

He gave the proof by Tchebychef⁷⁵ and his own proof.⁵⁷

J. T. Graves⁸⁰ employed $nx \equiv n+1 \pmod{p}$, where p is a prime, and stated that, for $n=1, \dots, p-1$, then $x \equiv 2, \dots, p$ in some order. Also $x \equiv p$ for $n=p-1$. Hence $2 \cdot 3 \cdot \dots (p-1) \equiv p-1 \pmod{p}$.

H. Durège⁸¹ obtained (2) for $a=x$ and Grunert's³⁶ results on the series $[m, n]$ by use of partial fractions for the reciprocal of $x(x-1)\dots(x-n)$.

E. Lottner⁸² employed for the same purpose infinite trigonometric and algebraic series, obtaining recursion formulæ for the coefficients.

⁷³Periodico Mensual Ciencias Mat. y Fis., Cadiz, 1, 1848, 63.

⁷⁴Bull. Ac. Sc. St. Pétersbourg, 6, 1848, 205.

⁷⁵Theorie der Congruenzen, 1849 (Russian); in German, 1889, §19. Same proof by J. A. Serret, Cours d'algèbre supérieure, ed. 2, 1854, 324.

⁷⁶Proc. Roy. Soc. London, 5, 1851, 664.

⁷⁷Théorie des nombres, Paris, 1852, 223-5.

^{77a}Jour. für Math., 44, 1852, 348.

⁷⁸Cambridge and Dublin Math. Jour., 9, 1854, 84; Coll. Math. Papers, 2, 1908, 10.

⁷⁹Einige Sätze aus den Anfangsgründen der Zahlenlehre, Progr. Realschule Posen, 1855.

⁸⁰British Assoc. Report, 1856, 1-3.

⁸¹Archiv Math. Phys., 30, 1858, 163-6.

⁸²*Ibid.*, 32, 1859, 111-5.

J. Toeplitz⁸³ gave Lagrange's proof of Wilson's theorem.

M. A. Stern⁸⁴ made use of the series for $\log(1-x)$ to show that

$$1+x+x^2+\dots=\frac{1}{1-x}=e^{x+x^2/2+x^3/3+\dots}.$$

Multiply together the series for e^x , $e^{x^2/2}$, etc. By the coefficient of x^p ,

$$1=\frac{1}{p!}+s+\frac{1}{p}, \quad s=\frac{1/2}{(p-2)!}+\dots$$

Take p a prime. No term of s has a factor p in the denominator. Hence

$$(1-s) \cdot (p-1)! = \frac{1+(p-1)!}{p} = \text{integer}.$$

V. A. Lebesgue⁸⁵ obtained Wilson's theorem by taking $x=p-1$ in

$$p \sum_{k=1}^x k(k+1) \dots (k+p-2) = x(x+1) \dots (x+p-1).$$

If P is a composite number $\neq 4$, $(P-1)!$ is divisible by P . He (p. 74) attributed Ivory's⁸³ proof of Fermat's theorem to Gauss, without reference.

G. L. Dirichlet⁸⁶ gave Horner's⁸⁷ and Euler's¹⁴ proof of Euler's theorem and derived it from Fermat's by the method of powering. His proof (§38) of the generalized Wilson theorem is by associated numbers, but is somewhat simpler than the analogous proofs.

Jean Plana⁸⁷ used the method of powering. Let $N=p^k p_1^{k_1} \dots$. For M prime to N , $M^{p-1} \equiv 1 + pQ$. Hence

$$M^{\varphi(p^k)} = (1+pQ)^{p^{k-1}} = 1 + p^k U, \quad M^{\varphi(p_1^{k_1})} = 1 + p_1^{k_1} U_1, \dots$$

Thus for $e = \varphi(p^k p_1^{k_1})$, $M^e - 1$ is divisible by p^k and $p_1^{k_1}$ and hence by their product, etc. Plana gave also a modification of Lagrange's proof of Wilson's theorem by use of (2); take $x=a=p-1$, subtract the expansion of $(1-1)^{p-1}$ and write the resulting series in reverse order:

$$(p-1)! + 1 = \binom{p-1}{2} (2^{p-1} - 1) - \binom{p-1}{3} (3^{p-1} - 1) + \dots \\ - \binom{p-1}{p-2} \{ (p-2)^{p-1} - 1 \} + \{ (p-1)^{p-1} - 1 \}.$$

H. F. Talbot⁸⁸ gave Euler's¹² proof of Fermat's theorem.

J. Blissard^{88a} proved the last statement of Euler.⁹

C. Sardi⁸⁹ gave Lagrange's proof of Wilson's theorem.

P. A. Fontebasso⁹⁰ proved (2) for $x=a$ by finding the first term of the a th order of differences of y^a , $(y+h)^a$, $(y+2h)^a$, ... and then setting $y=0$, $h=1$.

⁸³Archiv Math. Phys., 32, 1859, 104.

⁸⁴Lehrbuch der Algebraischen Analysis, Leipzig, 1860, 391.

⁸⁵Introd. théorie des nombres, Paris, 1862, 80, 17.

⁸⁶Zahlentheorie (ed. Dedekind), §§19, 20, 127, 1863; ed. 2, 1871; ed. 3, 1879, ed. 4, 1894.

⁸⁷Mem. Acad. Turin, (2), 20, 1863, 148-150.

⁸⁸Trans. Roy. Soc. Edinburgh, 23, 1864, 45-52.

^{88a}Math. Quest. Educ. Times, 6, 1866, 26-7.

⁸⁹Giornale di Mat., 5, 1867, 371-6.

⁹⁰Saggio di una introd. arit. trascendente, Treviso, 1867, 77-81.

C. A. Laisant and E. Beaujeux⁹¹ used the period $a_1 \dots a_n$ of the periodic fraction to base B for the irreducible fraction p_1/q , where q is prime to B . If p_2, \dots, p_n are the successive remainders,

$$Bp_1 = a_1q + p_2, \quad Bp_2 = a_2q + p_3, \dots, \quad Bp_n = a_nq + p_1.$$

Starting with the second equation, we obtain the period $a_2 \dots a_n a_1$ for p_2/q . Similarly for $p_3/q, \dots, p_n/q$. Thus the $f = \varphi(q)$ irreducible fractions with denominator q separate into sets of n each. Hence $f = kn$. Since $B^n \equiv 1, B' \equiv 1 \pmod{q}$.

L. Ottinger⁹² employed differential calculus to show that, in

$$P = (a+d)(a+2d) \dots \{a+(p-1)d\} = a^{p-1} + C_1^{p-1} a^{p-2} d + C_2^{p-1} a^{p-3} d^2 + \dots,$$

$$rC_r^{p-1} = \sum_{q=1}^r \frac{qp(p-1) \dots (p-q)}{q+1} C_{r-q}^{p-q-2} \quad (r \leq p-2),$$

C_r^k being the sum of the products of $1, 2, \dots, k$ taken r at a time. Hence, if p is a prime, C_r^{p-1} ($r=1, \dots, p-2$) is divisible by p , and

$$P \equiv a^{p-1} + d \cdot 2d \dots (p-1)d \pmod{p}.$$

For $a=d=1$, this gives $0 \equiv 1 + (p-1)! \pmod{p}$.

H. Anton⁹³ gave Gauss'²⁸ proof of Wilson's theorem.

J. Petersen⁹⁴ proved Wilson's theorem by dividing the circumference of a circle into p equal parts, where p is a prime, and marking the points $1, \dots, p$. Designate by $12 \dots p$ the polygon obtained by joining 1 with 2, 2 with 3, \dots , p with 1. Rearranging these numbers we obtain new polygons, not all convex. While there are $p!$ rearrangements, each polygon can be designated in $2p$ ways [beginning with any one of the p numbers as first and reading forward or backward], so that we get $(p-1)!/2$ figures. Of these $\frac{1}{2}(p-1)$ are regular. The others are congruent in sets of p , since by rotation any one of them assumes p positions. Hence p divides $(p-1)!/2 - (p-1)/2$ and hence $(p-2)! - 1$. Cf. Cayley¹⁰¹.

To prove Fermat's theorem, take p elements from q with repetitions in all ways, that is, in q^p ways. The q sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining $q^p - q$ sets are permuted in sets of p . Hence p divides $q^p - q$. [Cf. Perott,¹²⁶ Bricard.¹³¹]

F. Unferdinger⁹⁵ proved by use of series of exponentials that

$$z^n - \binom{m}{1}(z-1)^n + \binom{m}{2}(z-2)^n - \dots + (-1)^m \binom{m}{m}(z-m)^n$$

⁹¹Nouv. Ann. Math., (2), 7, 1868, 292-3.

⁹²Archiv Math. Phys., 48, 1868, 159-185.

⁹³Ibid., 49, 1869, 297-8.

⁹⁴Tidsskrift for Matematik, (3), 2, 1872, 64-65 (Danish).

⁹⁵Sitzungsberichte Ak. Wiss. Wien, 67, 1873, II, 363.

is zero if $n < m$, but, if $n \geq m$, equals

$$E_m + \binom{z-m}{1} E_{m+1} + \binom{z-m}{2} E_{m+2} + \dots + \binom{z-m}{n-m} E_n,$$

where

$$E_k = k^n - \binom{k}{1} (k-1)^n + \binom{k}{2} (k-2)^n - \dots + (-1)^{k-1} \binom{k}{k-1} 1^n.$$

For $n = m$, the initial sum equals $E_m = m!$.

P. Mansion⁹⁶ noted that Euler's theorem may be identified with a property of periodic fractions [cf. Laisant⁹¹]. Let N be prime to R . Taking R as the base of a scale of notation, divide $100\dots$ by N and let $q_1\dots q_n$ be the repetend. Then $(R^n - 1)/N = q_1\dots q_n$. Unless the n remainders r_i exhaust the integers $< N$ and prime to N , we divide $r_1' 00\dots$ by N , where r_1' is one of the integers distinct from the r_i , and obtain n new remainders r_i' . In this way it is seen that n divides $\varphi(N)$, so that N divides $R^{\varphi(N)} - 1$. [At bottom this is Euler's¹⁴ proof.]

P. Mansion⁹⁷ reproduced this proof, made historical remarks on the theorem and indicated an error by Poinso^t.⁶⁷

Franz Jorcke⁹⁸ reproduced Euler's²² proof of Wilson's theorem.

G. L. P. v. Schaewen⁹⁹ proved (2) with a changed to $-p$, by expanding the binomials.

Chr. Zeller¹⁰⁰ proved that, for $n \neq 4$,

$$n^x - (n-1)(n-1)^x + \binom{n-1}{2} (n-2)^x - \binom{n-1}{3} (n-3)^x + \dots$$

is divisible by n unless n is a prime such that $n-1$ divides x , in which case the expression is $\equiv -1 \pmod{n}$.

A. Cayley¹⁰¹ proved Wilson's theorem as had Petersen.⁹⁴

E. Schering¹⁰² took a prime to $m = 2^\pi p_1^{\pi_1} \dots p_\mu^{\pi_\mu}$, where the p 's are distinct odd primes and proved that $x^2 \equiv a \pmod{m}$ has roots if and only if a is a quadratic residue of each p_i and if $a \equiv 1 \pmod{4}$ when $\pi = 2$, $a \equiv 1 \pmod{8}$ when $\pi > 2$, and then has $\psi(m)$ roots, where $\psi(m) = 2^\mu$, $2^{\mu+1}$ or $2^{\mu+2}$, according as $\pi < 2$, $\pi = 2$, or $\pi > 2$. Let a be a fixed quadratic residue of m and denote the roots by $\pm a_j$ ($j = 1, \dots, \psi/2$). Set $a_j' = m - a_j$. The $\phi(m) - \psi(m)$ integers $< m$ and prime to m , other than the a_j , a_j' , may be denoted by a_j , a_j' ($j = \frac{1}{2}\psi + 1, \dots, \frac{1}{2}\phi$), where $a_j a_j' \equiv a \pmod{m}$. From the latter and $-a_j a_j' \equiv a$ ($j = 1, \dots, \psi/2$), we obtain, by multiplication,

$$a^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} r_1 \dots r_{\varphi} \pmod{m},$$

⁹⁶Messenger Math., 5, 1876, 33 (140); Nouv. Corresp. Math., 4, 1878, 72-6.

⁹⁷Théorie des nombres, 1878, Gand (tract).

⁹⁸Über Zahlkongruenzen, Progr. Fraustadt, 1878, p. 31.

⁹⁹Die Binomial Coefficienten, Progr. Saarbrücken, 1881, p. 20.

¹⁰⁰Bull. des sc. math. astr., (2), 5, 1881, 211-4.

¹⁰¹Messenger of Math., 12, 1882-3, 41; Coll. Math. Papers, 12, p. 45.

¹⁰²Acta Math., 1, 1882, 153-170; Werke, 2, 1909, 69-86.

where the r_j are the integers $< m$ and prime to m . Taking $a=1$, we have the generalized Wilson theorem. Applying a like argument when a is a quadratic non-residue of m [Minding⁴⁸], we get

$$a^{\frac{1}{2}\varphi(m)} \equiv r_1 \dots r_{\varphi} \equiv (-1)^{\frac{1}{2}\psi(m)} \pmod{m}.$$

This investigation is a generalization of that by Dirichlet.⁴⁰

E. Lucas¹⁰³ wrote X_p for $x(x+1)\dots(x+p-1)$, and Γ_p^q for the sum of the products of $1, \dots, p$ taken q at a time. Thus

$$x^p + \Gamma_{p-1}^1 x^{p-1} + \dots + \Gamma_{p-1}^{p-1} x = X_p.$$

Replacing p by $1, \dots, n$ in turn and solving, we get

$$x^n = X_n + \Delta_1 X_{n-1} + \dots + \Delta_{n-1} X_1,$$

where

$$(-1)^{n-p+1} \Delta_{n-p+1} = \begin{vmatrix} \Gamma^1 \Gamma^2 \dots \Gamma^{n-p+1} \\ 1 \Gamma^1 \dots \Gamma^{n-p} \\ \vdots \vdots \vdots \vdots \\ 0 \ 0 \dots 1 \ \Gamma^1 \end{vmatrix},$$

the subscript $p-1$ on the Γ 's being dropped. After repeating the argument by Tchebychef⁷⁵, Lucas noted that, if p is an odd prime, $\Delta_{n-p+1} \equiv 1$ or $0 \pmod{p}$, according as $p-1$ is or is not a divisor of n .

G. Wertheim¹⁰⁴ gave Dirichlet's⁸⁶ proof of the generalized Wilson theorem; also the first step in the proof by Arndt.⁷⁰

W. E. Heal¹⁰⁵ gave without reference Euler's¹⁴ proof.

E. Catalan¹⁰⁶ noted that if $2n+1$ is composite, but not the square of a prime, $n!$ is divisible by $2n+1$; if $2n+1$ is the square of a prime, $(n!)^2$ is divisible by $2n+1$.

C. Garibaldi¹⁰⁷ proved Fermat's theorem by considering the number N of combinations of ap elements p at a time, a single element being selected from each row of the table

$$\begin{array}{ccccccc} e_{11} & e_{12} & \dots & e_{1a} & & & \\ & \dots & \dots & \dots & & & \\ & & & e_{p1} & e_{p2} & \dots & e_{pa} \end{array}$$

From all possible combinations are to be omitted those containing elements from exactly n rows, for $n=1, \dots, p-1$. Let A_n denote the number of combinations p at a time of an elements forming n rows, such that in each combination occur elements from each row. Then

$$N = \binom{ap}{p} - \sum_{n=1}^{p-1} \binom{p}{n} A_n.$$

¹⁰³Bull. Soc. Math. France, 11, 1882-3, 69-71; Mathesis, 3, 1883, 25-8.

¹⁰⁴Elemente der Zahlentheorie, 1887, 186-7; Anfangsgründe der Zahlenlehre, 1902, 343-5 (331-2).

¹⁰⁵Annals of Math., 3, 1887, 97-98.

¹⁰⁶Mém. soc. roy. sc. Liège, (2), 15, 1888 (Mélanges Math., III, 1887, 139).

¹⁰⁷Giornale di Mat., 26, 1888, 197.

Take each $e_{ij}=1$; then $N=a^p$ since the number of the specified combinations becomes the sum of all products of p factors unity, one from each row of the table. Thus

$$a^p \equiv \binom{ap}{a} \equiv a \pmod{p}.$$

R. W. Genese¹⁰⁸ proved Euler's theorem essentially as did Laisant.⁹¹

M. F. Daniëls¹⁰⁹ proved the generalized Wilson theorem. If $\psi(n)$ denotes the product of the integers $< n$ and prime to n , he proved by induction that $\psi(p^\pi) \equiv -1 \pmod{p^\pi}$ for p an odd prime. For, if ρ_1, \dots, ρ_n are the integers $< p^\pi$ and prime to it, then $\rho_1 + jp^\pi, \dots, \rho_n + jp^\pi$ ($j=0, 1, \dots, p-1$) are the integers $< p^{\pi+1}$ and prime to it. He proved similarly by induction that $\psi(2^\pi) \equiv +1 \pmod{2^\pi}$ if $\pi > 2$. Evidently $\psi(2) \equiv 1 \pmod{2}$, $\psi(4) \equiv -1 \pmod{4}$. If $m=a^\alpha b^\beta \dots$ and $n=l^\lambda$, where l is a new prime, then $\psi(m) \equiv \epsilon \pmod{m}$, $\psi(n) \equiv \eta \pmod{n}$ lead by the preceding method to $\psi(mn) \equiv \epsilon^{\varphi(n)} \pmod{mn}$, viz., 1, unless $n=2$. The theorem now follows easily.

E. Lucas¹¹⁰ noted that, if x is prime to $n=AB\dots$, where A, B, \dots are powers of distinct primes, and if ϕ is the l. c. m. of $\phi(A), \phi(B), \dots$, then $x^\phi \equiv 1 \pmod{n}$. In case $A=2^k$, $k>2$, we may replace $\phi(A)$ by its half. To get a congruence holding whether or not x is prime to n , multiply the former congruence by x^σ , where σ is the greatest exponent of the prime factors of n . Note that $\phi+\sigma < n$ [Bachmann^{129, 143}]. Carmichael¹³⁹ wrote $\lambda(n)$ for ϕ .

E. Lucas¹¹¹ found $\Delta^{p-1}x^{p-1}$ in two ways by the theory of differences. Equating the two results, we have

$$(p-1)! = (p-1)^{p-1} - \binom{p-1}{1}(p-2)^{p-1} + \dots - \binom{p-1}{p-2}1^{p-1}.$$

Each power on the right is $\equiv 1 \pmod{p}$. Thus

$$(p-1)! \equiv (1-1)^{p-1} - 1 \equiv -1 \pmod{p}.$$

P. A. MacMahon¹¹² proved Fermat's theorem by showing that the number of circular permutations of p distinct things n at a time, repetitions allowed, is

$$\frac{1}{n} \sum \phi(d) p^{n/d},$$

where d ranges over the divisors of n . For n a prime, this gives

$$p^n + (n-1)p \equiv 0, \quad p^n \equiv p \pmod{n}.$$

Another specialization led to Euler's generalization.

E. Maillet¹¹³ applied Sylow's theorem on subgroups whose order is the highest power p^h of a prime p dividing the order m of a group, viz.,

¹⁰⁸British Association Report, 1888, 580-1.

¹⁰⁹Lineaire Congruenties, Diss. Amsterdam, 1890, 104-114.

¹¹⁰Bull. Ac. Sc. St. Pétersbourg, 33, 1890, 496.

¹¹¹Mathesis, (2), 1, 1891, 11; Théorie des nombres, 1891, 432.

¹¹²Proc. London Math. Soc., 23, 1891-2, 305-313.

¹¹³Recherches sur les substitutions, Thèse, Paris, 1892, 115.

$m = pN(1 + np)$, when $h = 1$. For the symmetric group on p letters, $m = p!$ and $N = p - 1$, so that $(p - 1)! \equiv -1 \pmod{p}$. There is exhibited a special group for which $m = pa^p$, $N = a$, whence $a^p \equiv a \pmod{p}$.

G. Levi¹¹⁴ failed in his attempt to prove Wilson's theorem. Let b and $a = (p - 1)b$ have the least positive residues r_1 and r when divided by p . Then $r + r_1 = p$. Multiply $b/p = q + r_1/p$ by $p - 1$. Thus $r_1(p - 1)$ has the same residue as a , so that

$$r_1(p - 1) = r + mp, \quad \frac{a}{p} = q(p - 1) + m + \frac{r}{p}.$$

He concluded that $r_1(p - 1) = r$, falsely, as the example $p = 5$, $b = 7$, shows. He added the last equation to $r + r_1 = p$ and concluded that $r_1 = 1$, $r = p - 1$, so that $(a + 1)/p$ is an integer. The fact that this argument is independent of Levi's initial choice that $b = (p - 2)!$ and his assumption that p is a prime shows that the proof is fallacious.

Axel Thue¹¹⁵ obtained Fermat's theorem by adding

$$a^p - (a - 1)^p = 1 + kp, \quad (a - 1)^p - (a - 2)^p = 1 + hp, \quad \dots, \quad 1^p - 0^p = 1$$

[Paoli¹¹⁶]. Then the differences $\Delta^1 F(j)$ of the first order of $F(x) = x^{p-1}$ are divisible by p for $j = 1, \dots, p - 2$; likewise $\Delta^2 F(1), \dots, \Delta^{p-2} F(1)$. By adding

$$\Delta^{j+1} F(0) = \Delta^j F(1) - \Delta^j F(0) \quad (j = 1, \dots, p - 2),$$

we get

$$-\Delta^{p-1} F(0) = 1 + \Delta^1 F(1) - \Delta^2 F(1) + \dots + \Delta^{p-2} F(1), \quad (p - 1)! + 1 \equiv 0 \pmod{p}.$$

N. M. Ferrers¹¹⁶ repeated Sylvester's⁷⁸ proof of Wilson's theorem.

M. d'Ocagne¹¹⁷ proved the identity in r :

$$(r + 1)^{k+1} + \frac{(k + 1)}{q!} \sum_{i=1}^q P_{k-1}^{(i-1)} P_q^{(q-i)} (r + 1)^{k+1-2i} (-r)^i \equiv r^{k+1} + 1,$$

where $q = [(k + 1)/2]$ and $P_m^{(n)}$ is the product of n consecutive integers of which m is the largest, while $P_n^0 = 1$. Hence if $k + 1$ is a prime, it divides $(r + 1)^{k+1} - r^{k+1} - 1$, and Fermat's theorem follows. The case $k = p - 1$ shows that if p is a prime, $q = (p - 1)/2$, and r is any integer,

$$\sum_{i=1}^q P_{p-2}^{(i-1)} P_q^{(q-i)} (r + 1)^{p-2i} (-r)^i \equiv 0 \pmod{q!}.$$

T. del Beccaro¹¹⁸ used products of linear functions to obtain a very complicated proof of the generalized Wilson theorem.

A. Schmidt¹¹⁹ regarded two permutations of $1, 2, \dots, p$ as identical if one is derived from the other by a cyclic substitution of its elements. From one of the $(p - 1)!$ distinct permutations he derived a second by adding

¹¹⁴Atti del R. Istituto Veneto di Sc., (7), 4, 1892-3, pp. 1816-42.

¹¹⁵Archiv Math. og Natur., Kristiania, 16, 1893, 255-265.

¹¹⁶Messenger Math., 23, 1893-4, 56.

¹¹⁷Jour. de l'école polyt., 64, 1894, 200-1.

¹¹⁸Atti R. Ac. Lincei (Fis. Mat.), 1, 1894, 344-371.

¹¹⁹Zeitschrift Math. Phys., 40, 1895, 124.

unity to each element and replacing $p+1$ by 1. Let m be the least number of repetitions of this process which will yield the initial permutation. For p a prime, $m=1$ or p . There are $p-1$ cases in which $m=1$. Hence $(p-1)! - (p-1)$ is divisible by p . Cf. Petersen.⁹⁴

Many proofs of (3), p. 63, have been given.¹²⁰

D. von Sterneck¹²¹ gave Legendre's proof of Wilson's theorem.

L. E. Dickson¹²² noted that, if p is a prime, $p(p-1)$ of the $p!$ substitutions on p letters have a linear representation $x' \equiv ax + b$, $a \not\equiv 0 \pmod{p}$, while the remaining ones are represented analytically by functions of degree > 1 which fall into sets of $p^2(p-1)$ each, viz., $af(x+b) + c$, where a is prime to p . Hence $p! - p(p-1)$ is a multiple of $p^2(p-1)$, and therefore $(p-1)! + 1$ is a multiple of p .

C. Moreau¹²³ gave without references Schering's¹⁰² extension to any modulus of Dirichlet's⁴⁰ proof of the theorems of Fermat and Wilson.

H. Weber¹²⁴ deduced Euler's theorem from the fact that the integers $< m$ and prime to m form a group under multiplication, whence every integer belongs to an exponent dividing the order $\phi(m)$ of the group.

E. Cahen¹²⁵ proved that the elementary symmetric functions of $1, \dots, p-1$ of order $< p-1$ are divisible by the prime p . Hence

$$(x-1)(x-2) \dots (x-p+1) \equiv x^{p-1} + (p-1)! \pmod{p},$$

identically in x . The case $x=1$ gives Wilson's theorem, so that also Fermat's theorem follows.

J. Perott¹²⁶ gave Petersen's⁹⁴ proof of Fermat's theorem, using q^p "configurations" obtained by placing the numbers $1, 2, \dots, q$ into p cases, arranged in a line. It is noted that the proof is not valid for p composite; for example, if $p=4$, $q=2$, the set of configurations derived from 1212 by cyclic permutations contains but one additional configuration 2121.

L. Kronecker¹²⁷ proved the generalized Wilson theorem essentially as had Brennecke.⁶⁷

G. Candido¹²⁸ made use of the identity

$$\begin{aligned} a^p + b^p &= (a+b)^p - pab(a+b)^{p-2} + \dots \\ &+ (-1)^r \frac{p(p-2r+1) \dots (p-r-1)}{1 \cdot 2 \dots r} a^r b^r (a+b)^{p-2r} + \dots \end{aligned}$$

Take p a prime and $b = -1$. Thus $a^p - a \equiv (a-1)^p - (a-1) \pmod{p}$.

¹²⁰L'intermédiaire des math., 3, 1896, 26-28, 229-231; 7, 1900, 22-30; 8, 1901, 164. A. Capelli
Giornale di Mat., 31, 1893, 310. S. Pincherle, *ibid.*, 40, 1902, 180-3.

¹²¹Monatshefte Math. Phys., 7, 1896, 145.

¹²²Annals of Math., (1), 11, 1896-7, 120.

¹²³Nouv. Ann. Math., (3), 17, 1898, 296-302.

¹²⁴Lehrbuch der Algebra, II, 1896, 55; ed. 2, 1899, 61.

¹²⁵Éléments de la théorie des nombres, 1900, 111-2.

¹²⁶Bull. des Sc. Math., 24, I, 1900, 175.

¹²⁷Vorlesungen über Zahlentheorie, 1901, I, 127-130.

¹²⁸Giornale di Mat., 40, 1902, 223.

P. Bachmann¹²⁹ proved the first statement of Lucas.¹¹⁰ He gave as a "new" proof of Euler's theorem (p. 320) the proof by Euler,¹⁴ and of the generalized Wilson theorem (p. 336) essentially the proof by Arndt.⁷⁰

J. W. Nicholson¹³⁰ proved the last formula of Grunert.³⁶

Bricard¹³¹ changed the wording of Petersen's⁹⁴ proof of Fermat's theorem. Of the q^p numbers with p digits written to the base q , omit the q numbers with a single repeated digit. The remaining $q^p - q$ numbers fall into sets each of p distinct numbers which are derived from one another by cyclic permutations of the digits.

G. A. Miller¹³² proved the generalized Wilson theorem by group theory. The integers relatively prime to g taken modulo g form under multiplication an abelian group of order $\phi(g)$ which is the group of isomorphisms of a cyclic group of order g . But in an abelian group the product of all the elements is the identity if and only if there is a single element of period 2. It is shown that a cyclic group is of order p^a , $2p^a$ or 4 if its group of isomorphisms contains a single element of period 2.

V. d'Escamard¹³³ reproduced Sylvester's⁷⁸ proof of Wilson's theorem.

K. Petr¹³⁴ gave Petersen's⁹⁴ proof of Wilson's theorem.

Prompt¹³⁵ gave an obscure proof that $2^{p-1} - 1$ is divisible by the prime p .

G. Arnoux¹³⁶ proved Euler's theorem. Let λ be any one of the $v = \phi(m)$ integers $\alpha, \beta, \gamma, \dots$, prime to m and $< m$. We can solve the congruences

$$\alpha\alpha' \equiv \beta\beta' \equiv \gamma\gamma' = \dots \equiv \lambda \pmod{m}.$$

Here α', β', \dots form a permutation of α, β, \dots . Thus

$$\alpha\alpha'\beta\beta' \dots \equiv (\alpha\beta \dots)^2 \equiv \lambda^v.$$

In particular, for $\lambda = 1$, we get $(\alpha\beta \dots)^2 \equiv 1$. Hence for any λ prime to m , $\lambda^v \equiv 1 \pmod{m}$. [Cf. Dirichlet,⁴⁰ Schering,¹⁰² C. Moreau.¹²³]

R. A. Harris^{136a} proved that $(\alpha\beta \dots)^2 \equiv 1$ as did Arnoux¹³⁶, but inferred falsely that $\alpha\beta \dots \equiv \pm 1$.

A. Aubry¹³⁷ started, as has Waring in 1782, with

$$x^n = Y_n + AY_{n-1} + \dots + MY_2 + Y_1,$$

where $Y_p = x(x-1) \dots (x-p+1)$. Then

$$x^{n+1} - x^n = Y_{n+1} + AY_n + \dots + MY_3 + Y_2.$$

Summing for $x = 1, \dots, p-1$ and setting $s_k = 1^k + 2^k + \dots + (p-1)^k$, we get

$$s_{n+1} - s_n = \frac{\{n+1\}}{n+2} + A \frac{\{n\}}{n+1} + \dots + \frac{M\{3\}}{4} + \frac{\{2\}}{3},$$

¹²⁹Niedere Zahlentheorie, I, 1902, 157-8.

¹³⁰Amer. Math. Monthly, 9, 1902, 187, 211.

¹³¹Nouv. Ann. Math., (4), 3, 1903, 340-2.

¹³²Annals of Math., (2), 4, 1903, 188-190. Cf. V. d'Escamard, Giornale di Mat., 41, 1903, 203-4; U. Scarpis, *ibid.*, 43, 1905, 323-8.

¹³³Giornale di Mat., 43, 1905, 379-380.

¹³⁴Casopis, Prag, 34, 1905, 164.

¹³⁵Remarques sur le théorème de Fermat, Grenoble, 1905, 32 pp.

¹³⁶Arithmétique Graphique; Fonctions Arith., 1906, 24.

^{136a}Math. Magazine, 2, 1904, 272.

¹³⁷L'enseignement math., 9, 1907, 434-5, 440.

where $\{k\} = p(p-1) \dots (p-k)$. Hence, if p is a prime and $n < p-1$, $s_{n+1} - s_n \equiv 0$. But $s_1 \equiv 0$. Hence $s_n \equiv 0 (n < p-1)$, $s_{p-1} \equiv -(p-1)!$. Thus Wilson's theorem follows from Fermat's.

Without giving references, Aubry (p. 298) attributed Horner's³⁷ proof of Euler's theorem to Gauss; the proof (pp. 439-440) by Paoli⁴⁶ (and Thue¹¹⁵) of Fermat's theorem to Euler¹²; the proof (p. 458) by Laplace²³ of Euler's theorem by powering to Euler.

R. D. Carmichael¹³⁸ noted that, if L is the l. c. m. of all the roots z of $\phi(z) = a$, and if x is prime to L , then $x^a \equiv 1 \pmod{L}$. Hence except when n and $n/2$ are the only numbers whose ϕ -function is the same as that of n , $x^{\phi(n)} \equiv 1$ holds for a modulus M which is some multiple of n . A practical method of finding M is given.

R. D. Carmichael¹³⁹ proved the first result by Lucas.¹¹⁰

J. A. Donaldson¹⁴⁰ deduced Fermat's theorem from the theory of periodic fractions.

W. A. Lindsay¹⁴¹ proved Fermat's theorem by use of the binomial theorem.

J. I. Tschistjakov¹⁴² extended Euler's theorem as had Lucas.¹¹⁰

P. Bachmann¹⁴³ proved the remarks by Lucas,¹¹⁰ but replaced $\phi + \sigma < n$ by $n \geq \phi + \sigma$, stating that the sign is $>$ if n is divisible by at least two distinct primes.

A. Thue¹⁴⁴ noted that a different kinds of objects can be placed into n given places in a^n ways. Of these let U_a^n be the number of placings such that each is converted into itself by not fewer than n applications of the operation which replaces each by the next and the last by the first. Then U_a^n is divisible by n . If n is a prime, $U_a^n = a^n - a$ and we have Fermat's theorem. Next, $a^n = \sum U_a^d$, where d ranges over the divisors of n . Finally, if p, q, \dots, r are the distinct prime factors of n ,

$$U_a^n = \sum (-1)^\theta a^{n/D} \equiv 0 \pmod{n},$$

where D ranges over the distinct divisors of $pq \dots r$, while θ is the number of prime factors of D . Euler's theorem is deduced from this.

H. C. Pocklington¹⁴⁵ repeated Bricard's¹³¹ proof.

U. Scarpis¹⁴⁶ proved the generalized Wilson theorem by a method similar to Arndt's.⁷⁰ The case of modulus 2^λ ($\lambda > 2$) is treated by induction. Assume that $\Pi r \equiv 1 \pmod{2^\lambda}$, where r_1, \dots, r_v are the $v = \phi(2^\lambda)$ odd integers $< 2^\lambda$. Then $r_1, \dots, r_v, r_1 + 2^\lambda, \dots, r_v + 2^\lambda$ are the residues modulo $2^{\lambda+1}$ and their product is seen to be $\equiv 1 \pmod{2^{\lambda+1}}$. Next, let the modulus be

¹³⁸Bull. Amer. Math. Soc., 15, 1908-9, 221-2.

¹³⁹*Ibid.*, 16, 1909-10, 232-3.

¹⁴⁰Edinburgh Math. Soc. Notes, 1909-11, 79-84.

¹⁴¹*Ibid.*, 78-79.

¹⁴²Tagbl. XII Vers. Russ. Nat., 124, 1910 (Russian).

¹⁴³Niedere Zahlentheorie, II, 1910, 43-44.

¹⁴⁴Skrifter Videnskabs-Selskabet, Christiania, 1910, No. 3, 7 pp.

¹⁴⁵Nature, 84, 1910, 531.

¹⁴⁶Periodico di Mat., 27, 1912, 231-3.

$n = p_1^{a_1} \dots p_h^{a_h}$ ($h > 2$), $n \neq 2p^\lambda$. Then a system of residues modulo n , each prime to n , is given by $\sum_{i=1}^h A_i r_i$, with

$$A_i = \left(\frac{n}{p_i^{a_i}} \right)^{\phi(p_i^{a_i})},$$

where r_i ranges over a system of residues modulo $p_i^{a_i}$, each prime to p_i . Let P be the product of these $\sum A_i r_i$. Since $A_i A_j$ is divisible by n if $i \neq j$,

$$P \equiv \sum_{i=1}^h A_i^{\varphi(n)} (\prod r_i)^{\varphi(n/p_i^{a_i})} \pmod{n}.$$

Thus $P-1$ is divisible by each $p_k^{a_k}$ and hence by n .

*Illgner¹⁴⁷ proved Fermat's theorem.

A. Bottari¹⁴⁸ proved Wilson's theorem by use of a primitive root [Gauss³⁰].

J. Schumacher¹⁴⁹ reproduced Cayley's¹⁰¹ proof of Wilson's theorem.

A. Arévalo¹⁵⁰ employed the sum S_n of the products taken n at a time of $1, 2, \dots, p-1$. By the known formula

$$S_n = \frac{1}{n} \left\{ \binom{p}{n+1} + \binom{p-1}{n} S_1 + \binom{p-2}{n-1} S_2 + \dots + \binom{p-n+1}{2} S_{n-1} \right\},$$

it follows by induction that S_n is divisible by the prime p if $n < p-1$. In the notation of Wronski, write $a^{p/r}$ for

$$a(a+r) \dots \{a+(p-1)r\} = a^p + S_1 a^{p-1} r + \dots + S_{p-1} a r^{p-1}.$$

For $a=r=1$, we have $p! = 1 + S_1 + \dots + S_{p-1}$, whence $S_{p-1} \equiv -1 \pmod{p}$, giving Wilson's theorem. Also, $a^{p/r} \equiv a^p - a \cdot r^{p-1}$. Dividing by a and taking $r=1$, we have

$$(a+1)^{(p-1)/1} \equiv a^{p-1} - 1 \pmod{p}.$$

The left member is divisible by p if a is not. Hence we have Fermat's theorem. Another proof follows from Vandermonde's formula

$$(x+a)^{p/r} = \sum_{h=0}^p \binom{p}{h} x^{(p-h)/r} a^{h/r} \equiv x^{p/r} + a^{p/r} \pmod{p},$$

$$(x_1 + \dots + x_a)^{p/r} \equiv x_1^{p/r} + \dots + x_a^{p/r}, \quad a^{p/r} \equiv a \cdot 1^{p/r}.$$

Remove the factor a and set $r=0$; we obtain Fermat's theorem.

Prompt¹⁵¹ gave Euler's¹⁴ proof of his theorem and two proofs of the type sketched by Gauss of his generalization of Wilson's theorem; but obscured the proofs by lengthy numerical computations and the use of unconventional notations.

F. Schuh¹⁵² proved Euler's theorem, the generalized Wilson theorem, and discussed the symmetric functions of the roots of a congruence for a prime modulus.

¹⁴⁷Lehrsatz über $x^n - x$, Unterrichts Blätter für Math. u. Naturwiss., Berlin, 18, 1912, 15.

¹⁴⁸Il Boll. Matematica Gior. Sc.-Didat., 11, 1912, 289.

¹⁴⁹Zeitschrift Math.-naturwiss. Unterricht, 44, 1913, 263-4.

¹⁵⁰Revista de la Sociedad Mat. Española, 2, 1913, 123-131.

¹⁵¹Démonstrations nouvelles des théorèmes de Fermat et de Wilson, Paris, Gauthier-Villars, 1913, 18 pp. Reprinted in l'intermédiaire des math., 20, 1913, end.

¹⁵²Suppl. de Vriend der Wiskunde, 25, 1913, 33-59, 143-159, 228-259.

G. Frattini¹⁵³ noted that, if $F(a, \beta, \dots)$ is a homogeneous symmetric polynomial, of degree g with integral coefficients, in the integers a, β, \dots less than m and prime to m , and if F is prime to m , then $k^g \equiv 1 \pmod{m}$ for every integer k prime to m . In fact,

$$F(a, \beta, \dots) \equiv F(ka, k\beta, \dots) \equiv k^g F(a, \beta, \dots) \pmod{m}.$$

Taking F to be the product $a\beta \dots$, we have Euler's theorem. Another corollary is

$$\prod_{j=1}^{p-1} (1+j) \equiv 1 + (p-1)! \pmod{p},$$

for p a prime, which implies Wilson's theorem.

*J. L. Wildschütz-Jessen¹⁵⁴ gave an historical account of Fermat's and Wilson's theorems.

E. Piccioli¹⁵⁵ repeated the work of Dirichlet.⁴⁰

THE GENERALIZATION $F(a, N) \equiv 0 \pmod{N}$ OF FERMAT'S THEOREM.

C. F. Gauss¹⁶⁰ noted that, if $N = p_1^{e_1} \dots p_s^{e_s}$ (p 's distinct primes),

$$F(a, N) = a^N - \sum_{i=1}^s a^{N/p_i} + \sum_{i < j} a^{N/p_i p_j} - \sum_{i < j < k} a^{N/p_i p_j p_k} + \dots + (-1)^s a^{N/p_1 \dots p_s}$$

is divisible by N when a is a prime, the quotient being the number of irreducible congruences modulo a of degree N and highest coefficient unity. He proved that

$$(1) \quad a^N = \sum F(a, d), \quad F(a, 1) = a,$$

where d ranges over all the divisors of N , and stated that this relation readily leads to the above expression for $F(a, N)$. [See Ch. XIX on inversion.]

Th. Schönemann¹⁶¹ gave the generalization that if a is a power p^n of a prime, the number of congruences of degree N irreducible in the Galois field of order a is $N^{-1}F(a, N)$.

An account of the last two papers and later ones on irreducible congruences will be given in Ch. VIII.

J. A. Serret¹⁶² stated that, for any integers a and N , $F(a, N)$ is divisible by N . For $N = p^e$, p a prime, this implies that

$$a^{\phi(p^e)} \equiv 1 \pmod{p^e},$$

when a is prime to p , a case of Euler's theorem.

S. Kantor¹⁶³ showed that the number of cyclic groups of order N in any birational transformation of order a in the plane is $N^{-1}F(a, N)$. He obtained (1) and then the expression for $F(a, N)$ by a lengthy method completed for special cases.

¹⁵³Periodico di Mat., 29, 1913, 49-53.

¹⁵⁴Nyt Tidsskrift for Mat., 25, A, 1914, 1-24, 49-68 (Danish).

¹⁵⁵Periodico di Mat., 32, 1917, 132-4.

¹⁶⁰Posthumous paper, Werke, 2, 1863, 222; Gauss-Maser, 611.

¹⁶¹Jour. für Math., 31, 1846, 269-325. Progr. Brandenburg, 1844.

¹⁶²Nouv. Ann. Math., 14, 1855, 261-2.

¹⁶³Annali di Mat., (2), 10, 1880, 64-73. Comptes Rendus Paris, 96, 1883, 1423.

Ed. Weyr¹⁶⁴, E. Lucas¹⁶⁵, and Pellet¹⁶⁵ gave direct proofs that $F(a, N)$ is divisible by N for any integers a, N .

H. Picquet¹⁶⁶ noted the divisibility of $F(3m-1, N)$ by N in an enumeration of certain curvilinear polygons of N sides, at the same time inscribed and circumscribed in a given cubic curve. He gave a proof of the divisibility of $F(a, N)$ by N , requiring various subcases. He stated that the function $F(a, N)$ is characterized by the two relations

$$(2) \quad F(a, np^s) = F(a^{p^s}, n) - F(a^{p^{s-1}}, n), \quad F(a, p^s) = a^{p^s} - a^{p^{s-1}},$$

where a is any integer, n an integer not divisible by the prime p .

A. Grandi¹⁶⁷ proved that $F(a, N)$ is divisible by N by writing it as

$$a^N - a^{N/p_1} - \{ (a^{N/p_2} - a^{N/p_1 p_2}) + (a^{N/p_3} - a^{N/p_2 p_3}) + \dots \} \\ + \{ (a^{N/p_2 p_3} - a^{N/p_1 p_2 p_3}) + \dots \} + \dots$$

Each of these binomials is divisible by $p_1^{e_1}$ since

$$a^{(p-1)p^{e-1}} \equiv 1, \quad a^{p^e} \equiv a^{p^{e-1}} \pmod{p^e}.$$

G. Koenigs¹⁶⁸ considered a uniform substitution $z' = \phi(z)$ and its n th power $z'' = \phi_n(z)$. Those roots of $z - \phi_n(z) = 0$ which satisfy no like equation of lower index are said to belong to the index n . If x belongs to the index n , so do also $\phi_i(x)$ for $i=1, \dots, n-1$. Thus the roots belonging to the index n are distributed into sets of n . If a is the degree of the polynomials in the numerator and denominator of $\phi(z)$, the number of roots belonging to the index n is $F(a, n)$, which is therefore divisible by n .

MacMahon's¹¹² paper contains in a disguised form the fact that $F(a, N)$ is divisible by N . Proofs were given by E. Maillet¹¹³ by substitution groups, and by G. Cordone.¹⁶⁹

Borel and Drach¹⁷⁰ made use of Gauss' result that $F(p, N)$ is divisible by N for every prime p and integer N , and Dirichlet's theorem that there exist an infinitude of primes p congruent modulo N to any given integer a prime to N , to conclude that $F(a, N)$ is divisible by N .

L. E. Dickson¹⁷¹ proved by induction (from k to $k+1$ primes) that $F(a, N)$ is characterized by properties (2) and concluded by induction that $F(a, N)$ is divisible by N . A like conclusion was drawn from

$$\{F(a, N)\}^q - F(a, N) \equiv F(a, qN) \pmod{q},$$

where q is a prime. He gave the relations

$$F(a, nN) = F(a^N, n) - \sum_{i=1}^s F(a^{N/p_i}, n) + \sum_{i < j} F(a^{N/p_i p_j}, n) - \dots \\ + (-1)^s F(a^{N/p_1 \dots p_s}, n), \\ F(a, N) = \sum \phi(d),$$

¹⁶⁴Casopis, Prag, 11, 1882, 39.

¹⁶⁵Comptes Rendus Paris, 96, 1883, 1300-2.

¹⁶⁶*Ibid.*, p. 1136, 1424. Jour. de l'école polyt., cah. 54, 1884, 61, 85-91.

¹⁶⁷Atti R. Istituto Veneto di Sc., (6), 1, 1882-3, 809.

¹⁶⁸Bull. des sciences math., (2), 8, 1884, 286.

¹⁶⁹Rivista di Mat., Torino, 5, 1895, 25.

¹⁷⁰Introd. théorie des nombres, 1895, 50.

¹⁷¹Annals of Math., (2), 1, 1899, 35. Abstr. in Comptes Rendus Paris, 128, 1899, 1083-5.

where d ranges over those divisors of $a^N - 1$ which do not divide $a^v - 1$ for $0 < v < N$; while, in the former, p_1, \dots, p_s are the distinct prime factors of N , and n is prime to N .

L. Gegenbauer¹⁷² wrote $F(a, n)$ in the form $\sum \mu(d) a^{n/d}$, where d ranges over the divisors of n , and $\mu(d)$ is the function discussed in Chapter XIX on Inversion. As there shown, $\sum \mu(d) = 0$ if $n > 1$. This case $f(x) = \mu(x)$ is used to prove the generalization: If the function $f(x)$ has the property that $\sum f(d)$ is divisible by n , then for every integer a the function $\sum f(d) a^{n/d}$ is divisible by n , where in each sum d ranges over the divisors of n . Another special case, $f(x) = \phi(x)$, was noted by MacMahon.¹¹²

J. Westlund¹⁷³ considered any ideal A in a given algebraic number field, the distinct prime factors P_1, \dots, P_i of A , the norm $n(A)$ of A , and proved that if a is any algebraic integer,

$$a^{n(A)} - \sum a^{n(A)/n(P_1)} + \sum a^{n(A)/n(P_1 P_2)} - \dots + (-1)^i a^{n(A)/n(P_1 \dots P_i)}$$

is always divisible by A .

J. Vályi¹⁷⁴ noted that the number of triangles similar to their n th pedal but not to the d th pedal ($d < n$) is

$$\chi(n) = \psi(n) - \sum \psi\left(\frac{n}{p_1}\right) + \sum \psi\left(\frac{n}{p_1 p_2}\right) - \dots,$$

if p_1, p_2, \dots are the distinct prime factors of n , and $\psi(k) = 2^k(2^k - 1)$. He proved that $\chi(n)$ is divisible by n , since if the n th pedal to ABC is the first one similar to ABC , a like property is true of the first pedal, \dots , $(n-1)$ th pedal, so that the $\chi(n)$ triangles fall into sets of n each of period n . [Note that $\chi(n) = F(4, n) - F(2, n)$.]

A. Axer¹⁷⁵ proved the following generalization of Gegenbauer's¹⁷² theorem: If $G(r_1, \dots, r_h)$ is any polynomial with integral coefficients, and if, when d ranges over all the divisors of n ,

$$\sum f(d) G(r_1^{n/d}, \dots, r_h^{n/d}) \equiv 0 \pmod{n}$$

for a particular function $G = G_0$ and a particular set of values r_{10}, \dots, r_{h0} , not a set of solutions of G_0 , and for which G_0 is prime to n , then it holds for every G and every set r_1, \dots, r_h .

FURTHER GENERALIZATIONS OF FERMAT'S THEOREM.

For the generalization to Galois imaginaries, see Ch. VIII.

For the generalization by Lucas, see Ch. XVII, Lucas,³⁹ Carmichael.⁸⁹

On $x^J \equiv 1 \pmod{n}$ for x prime to n , see Cauchy,²⁶ Moreau,⁹³ Epstein,¹¹² of Ch. VII.

O. H. Mitchell¹⁷⁸ considered the 2^i products s of distinct primes dividing $k = p_1^{e_1} \dots p_i^{e_i}$ and denoted by $\tau_s(k)$ the number of positive integers $X_s < k$ which are divisible by s but by no prime factor of k not dividing s .

¹⁷²Monatshefte Math. Phys., 11, 1900, 287-8.

¹⁷³Proc. Indiana Ac. Sc., 1902, 78-79.

¹⁷⁴Monatshefte Math. Phys., 14, 1903, 243-253.

¹⁷⁵Monatshefte Math. Phys., 22, 1911, 187-194.

¹⁷⁸Amer. Jour. Math., 3, 1880, 300; Johns Hopkins Univ. Circular, 1, 1880-1, 67, 97.

The products of the various X_s by any one of them are congruent modulo k to the X_s in some order. Hence

$$X_s^{\tau_s(k)} \equiv R_s \pmod{k},$$

where R_s is the corresponding one of the 2^i roots of $x^2 \equiv x \pmod{k}$. The analogous extension of Wilson's theorem is $\prod X_s \equiv \pm R_s \pmod{k}$, the sign being minus only when $k/\sigma = p^\pi$, $2p^\pi$ or 4 and at the same time σ/s is odd. Here $\sigma = \prod p_j^{e_j}$ if $s = \prod p_j$. Cf. Mitchell,⁵⁰ Ch. V.

F. Rogel¹⁷⁹ proved that, if p is a prime not dividing n ,

$$n^{p-1} = 1 + \binom{p}{1}(n-1) + \binom{p}{2}(n-1)^2 + \dots + \binom{p}{k}(n-1)^k + \rho, \quad k = \frac{p-1}{2},$$

where ρ is divisible by every prime lying between k and $p+1$.

Borel and Drach¹⁸⁰ investigated the most general polynomial in x divisible by m for all integral values of x , but not having all its coefficients divisible by m . If $m = p^a q^b, \dots$, where p, q, \dots are distinct primes, and if $P(x), Q(x), \dots$ are the most general polynomials divisible by p^a, q^b, \dots , respectively, that for m is evidently

$$\{P(x) + p^a f(x)\} \{Q(x) + q^b g(x)\} \dots$$

For $a < p+1$, the most general $P(x)$ is proved to be

$$\sum_{k=1}^a f_k(x) \phi_k(x), \quad \phi_k(x) = p^{a-k} (x^p - x)^k,$$

where the f 's are arbitrary polynomials. For $a < 2(p+1)$, the most general $P(x)$ is

$$\sum_{k=1}^a f_k \phi_k + \sum_{k=1}^{a-p} \psi_k g_k, \quad \psi_k = \phi(x) (x^p - x)^{k-1} p^{a-p-k},$$

where $\phi(x) = (x^p - x)^p - p^{p-1} (x^p - x)$, and the f 's, g 's are arbitrary polynomials. Note that $\phi^p(x) - p^{p^2-1} \phi(x)$ is divisible by p^{p^2+p+1} . Cf. Nielsen.¹⁹⁴

E. H. Moore¹⁸¹ proved the generalization of Fermat's theorem:

$$\begin{vmatrix} x_1^{pm-1} & \dots & x_m^{pm-1} \\ \dots & \dots & \dots \\ x_1^p & \dots & x_m^p \\ x_1 & \dots & x_m \end{vmatrix} \equiv \prod_{k=1}^m \prod_{c_k+1=0}^{p-1} \dots \prod_{c_m=0}^{p-1} (x_k + c_{k+1}x_{k+1} + \dots + c_mx_m) \pmod{p}.$$

F. Gruber¹⁸² showed that, if n is composite and a_1, \dots, a_t are the $t = \phi(n)$ integers $< n$ and prime to n , the congruence

$$(1) \quad x^t - 1 \equiv (x - a_1) \dots (x - a_t) \pmod{n}$$

is an identity in x if and only if $n = 4$ or $2p$, where p is a prime $2^i + 1$.

¹⁷⁹Archiv Math. Phys., (2), 10, 1891, 84-94 (210).

¹⁸⁰Introduction théorie des nombres, 1895, 339-342.

¹⁸¹Bull. Amer. Math. Soc., 2, 1896, 189; cf. 13, 1906-7, 280.

¹⁸²Math. Nat. Berichte aus Ungarn, 13, 1896, 413-7; Math. termés ertesito, 14, 1896, 22-25.

E. Malo¹⁸³ employed integers A_i' and set $u = x^\mu z$,

$$z = \sum A_i' x^i, \quad z^k = \sum A_i^{(k)} x^i, \quad \theta = \frac{u^{n-1} du}{1-u^\mu} = \sum \omega_p x^{p-1} dx.$$

Since $\int_0^u \theta = \sum u^k/k$ ($k = n, m+n, 2m+n, \dots$),

$$\sum \frac{\omega_p}{p} x^p = \sum \frac{x^{\mu k} z^k}{k}, \quad \frac{\omega_p}{p} = \sum \frac{1}{k} A_{p-\mu k}^{(k)},$$

where k takes the values $n, m+n, \dots$ which are $\leq p/\mu$. If no prime factor of such a k occurs in the denominator of the expansion of ω_p/p , the latter is an integer; this is the case if p is a prime and $\mu \geq 2$. For $m = n = 1$, $\mu = 2$,

$$z(1-x)^a = \binom{a}{2} - \binom{a}{3}x + \dots \mp ax^{a-3} \pm x^{a-2},$$

we get $\omega_p = a^p - a$ and hence Fermat's theorem.

L. Kronecker¹⁸⁴ generalized Fermat's and Wilson's theorems to modular systems.

R. Le Vavasseur¹⁸⁵ obtained a result evidently equivalent to that by Moore¹⁸¹ for the non-homogeneous case $x_m = 1$.

M. Bauer¹⁸⁶ proved that if $n = p^\pi m$, where m is not divisible by the odd prime p , and a_1, \dots, a_t are the $t = \phi(n)$ integers $< n$ and prime to n ,

$$(x - a_1) \dots (x - a_t) \equiv (x^{p-1} - 1)^{t/(p-1)} \pmod{p^\pi},$$

identically in x . If $p = 2$ and $\pi > 1$, the product is identically congruent to $(x^2 - 1)^{t/2}$. Hence he found the values of d, n for which (1) holds modulo d , when d is a divisor of n . If p denotes an odd prime and q a prime $2^i + 1$, the values are

$$\begin{array}{c|c|c|c|c} d & 2q & 4 & p & 2 \\ \hline n & 2q & 4 & p^a, 2p^a & 2^a, 2^a q_1 q_2 \dots \end{array}.$$

M. Bauer¹⁸⁷ determined how n and N must be chosen so that $x^n - 1$ shall be congruent modulo N to a product of linear functions. We may restrict N to the case of a power of a prime. If p is an odd prime, $x^n - 1$ is congruent modulo p^a to a product of linear functions only when $p \equiv 1 \pmod{n}$, a arbitrary, or when $n = p^\pi m$, $a = 1$, $p \equiv 1 \pmod{m}$. For $p = 2$, only when $n = 2^\beta$, $a = 1$, or $n = 2$, a arbitrary. For the case n a prime, the problem was treated otherwise by Perott.¹⁸⁸

M. Bauer¹⁸⁹ noted that, if $n = p^\pi m$, where m is not divisible by the odd prime p ,

$$\prod_{i=1}^n (x - i) \equiv (x^p - x)^{n/p} \pmod{p^\pi}.$$

¹⁸³L'intermédiaire des math., 7, 1900, 281, 312.

¹⁸⁴Vorlesungen über Zahlentheorie, I, 1901, 167, 192, 220-2.

¹⁸⁵Comptes Rendus Paris, 135, 1902, 949; Mém. Ac. Sc. Toulouse, (10), 3, 1903, 39-48.

¹⁸⁶Nouv. Ann. Math., (4), 2, 1902, 256-264.

¹⁸⁷Math. Nat. Berichte aus Ungarn, 20, 1902, 34-38; Math. és Phys. Lapok, 10, 1901, 274-8 (pp. 145-152 relate to the "theory of Fermat's congruence"; no report is available).

¹⁸⁸Amer. Jour. Math., 11, 1888; 13, 1891.

¹⁸⁹Math. és Phys. Lapok, 12, 1903, 159-160.

Richard Sauer¹⁹⁰ proved that, if $a, b, a-b$ are prime to k ,

$$a^\varphi + a^{\varphi-1}b + a^{\varphi-2}b^2 + \dots + b^\varphi \equiv 1 \pmod{k}, \quad \varphi = \varphi(k),$$

since $a^{\varphi+1} - b^{\varphi+1} \equiv a - b$. Changing alternate signs to minus, we have a congruence valid if a, b are prime to k , and if $a+b$ is not divisible by k . If p is an odd prime dividing $a \mp b$,

$$a^{p-1} \pm a^{p-2}b + \dots + b^{p-1}$$

is divisible by p , but not by p^2 .

A. Capelli¹⁹¹ showed that, if a, b are relatively prime,

$$\frac{a^{\varphi(b)} + b^{\varphi(a)} - 1}{ab} = \left[\frac{a^{\varphi(b)-1}}{b} \right] + \left[\frac{b^{\varphi(a)-1}}{a} \right] + 1,$$

where $[x]$ is the greatest integer $\leq x$.

M. Bauer¹⁹² proved that, if p is an odd prime and $m = p^a$ or $2p^a$, every integer x relatively prime to m satisfies the congruence

$$(x^{p-1} - 1)^{p^{a-1}} \equiv (x+k_1) \dots (x+k_l) \pmod{m},$$

where k_1, \dots, k_l denote the $l = \phi(m)$ integers $< m$ and prime to $m > 2$. If m is not 4, p^a or $2p^a$, every integer x prime to m satisfies the congruence

$$(x^{\varphi(m)/2} - 1)^2 \equiv (x+k_1) \dots (x+k_l) \pmod{m}.$$

L. E. Dickson¹⁹³ proved Moore's¹⁸¹ theorem by invariantive theory.

N. Nielsen¹⁹⁴ proved that, if $\Phi(x)$ is a polynomial with integral coefficients not having a common factor > 1 , and if for every integral value of x the value of $\Phi(x)$ is divisible by the positive integer m , then

$$\Phi(x) = \phi(x) \omega_p(x) + \sum_{s=1}^{p-1} m_{p-s} A_s \omega_s(x), \quad \omega_n(x) \equiv x(x+1) \dots (x+n-1),$$

where $\phi(x)$ is a polynomial with integral coefficients, the A_s are integers, p is the least positive integer for which $p!$ is divisible by m , and m_{p-s} is the least positive integer l for which $s!l$ is divisible by m . Cf. Borel and Drach.¹⁸⁰

H. S. Vandiver¹⁹⁵ proved that, if V ranges over a complete set of incongruent residues modulo $m = p_1^{a_1} \dots p_k^{a_k}$, while U ranges over those V 's which are prime to m ,

$$\Pi(x-V) \equiv \sum_{s=1}^k t_s (x^{p_s} - x)^{m/p_s}, \quad \Pi(x-U) \equiv \sum t_s (x^{p_s-1} - 1)^{\varphi(m)/(p_s-1)},$$

modulo m , where $t_s = (m/p_s^{a_s})^e$, $e = \phi(p_s^{a_s})$. For $m = p^a$, the second congruence is due to Bauer.^{186, 192}

¹⁹⁰Eine polynomische Verallgemeinerung des Fermatschen Satzes, Diss., Giessen, 1905.

¹⁹¹Dritter Internat. Math. Kongress, Leipzig, 1905, 148-150.

¹⁹²Archiv Math. Phys., (3), 17, 1910, 252-3. Cf. Bouniakowsky³⁸ of Ch. XI.

¹⁹³Trans. Amer. Math. Soc., 12, 1911, 76; Madison Colloquium of the Amer. Math. Soc., 1914, 39-40.

¹⁹⁴Nieuw Archief voor Wiskunde, (2), 10, 1913, 100-6.

¹⁹⁵Annals of Math., (2), 18, 1917, 119.

FURTHER GENERALIZATIONS OF WILSON'S THEOREM; RELATED PROBLEMS.

J. Steiner²⁰⁰ proved that, if A_k is the sum of all products of powers of a_1, a_2, \dots, a_{p-k} of degree k , and the a 's have incongruent residues $\not\equiv 0$ modulo p , a prime, then A_1, \dots, A_{p-2} are divisible by p .

He first showed by induction that

$$\begin{aligned} x^{p-1} &= X_{p-1} + A_1 X_{p-2} + \dots + A_{p-2} X_1 + A_{p-1}, \\ X_k &\equiv (x-a_1) \dots (x-a_k), \quad A_1 = a_1 + \dots + a_{p-1}, \\ A_2 &= a_1^2 + a_1 a_2 + \dots + a_1 a_{p-2} + a_2^2 + a_2 a_3 + \dots + a_{p-2}^2, \dots \end{aligned}$$

For example, to obtain x^3 he multiplied the respective terms of

$$x^2 = (x-a_1)(x-a_2) + (a_1+a_2)(x-a_1) + a_1^2$$

by $x, (x-a_3)+a_3, (x-a_2)+a_2, (x-a_1)+a_1$. Let a_1, \dots, a_{p-1} have the residues $1, \dots, p-1$ in some order, modulo p . For $x-a_2$ divisible by p , $x^{p-1} \equiv A_{p-1} = a_1^{p-1} \pmod{p}$, so that $A_{p-2} X_1$ and hence also A_{p-2} is divisible by p . Then for $x \equiv a_3$, $A_{p-3} X_2$ and A_{p-3} are divisible by p . For $x=0$, $a_1=1$, the initial equation yields Wilson's theorem.

C. G. J. Jacobi²⁰¹ proved the generalization: If a_1, \dots, a_n have distinct residues $\not\equiv 0$, modulo p , a prime, and P_{nm} is the sum of their multiplicative combinations with repetitions m at a time, P_{nm} is divisible by p for $m = p-n, p-n+1, \dots, p-2$.

Note that Steiner's A_k is $P_{p-k, k}$. We have

$$(1) \quad \frac{1}{(x-a_1) \dots (x-a_n)} = \frac{1}{x^n} + \frac{P_{n1}}{x^{n+1}} + \frac{P_{n2}}{x^{n+2}} + \dots, \quad P_{nm} = \sum_{j=1}^n a_j^{n+m-1} / D_j,$$

$$D_j = (a_j - a_1) \dots (a_j - a_{j-1})(a_j - a_{j+1}) \dots (a_j - a_n), \quad 0 = \sum_{j=1}^n a_j^k / D_j \quad (k < n-1).$$

Let $n+m-1 = k + \beta(p-1)$. Then $a_j^{n+m-1} \equiv a_j^k \pmod{p}$. Hence if $k < n-1$,

$$D_1 \dots D_n P_{nm} \equiv D_1 \dots D_n \sum a_j^k / D_j, \quad P_{nm} \equiv 0 \pmod{p}.$$

The theorem follows by taking $\beta=1$ and $k=0, 1, \dots, n-2$ in turn.

H. F. Scherk²⁰² gave two generalizations of Wilson's theorem. Let p be a prime. By use of Wilson's theorem it is easily proved that

$$(p-n-1)! \equiv (-1)^n \frac{px-1}{n!} \pmod{p},$$

where x is an integer such that $px \equiv 1 \pmod{n!}$. Next, let C_k^r denote the sum of the products of $1, 2, \dots, k$ taken r at a time with repetitions. By use of partial fractions it is proved that

$$(p-r-1)! C_{p-r-1}^r + (-1)^r \equiv 0 \pmod{p} \quad (r < p-1).$$

It is stated that

²⁰⁰Jour. für Math., 13, 1834, 356; Werke 2, p. 9.

²⁰¹Ibid., 14, 1835, 64-5; Werke 6, 252-3.

²⁰²Bericht über die 24. Versammlung Deutscher Naturforscher und Aerzte in 1846, Kiel, 1847, 204-208.

$$C_{p-r-1}^r C_r^{p-r-1} + (-1)^r \equiv 0, \quad C_m^m - m! \equiv 0 \pmod{p}, \quad m = \frac{p-1}{2}.$$

H. F. Scherk²⁰³ proved Jacobi's theorem and the following: Form the sum P_{nh} of the multiplicative combinations with repetitions of the h th class of any n numbers less than the prime p , and the sum of the combinations without repetitions out of the remaining $p-n-1$ numbers $< p$; then the sum or the difference of the two is divisible by p according as h is odd or even.

Let C_k^h denote the sum of the combinations with repetitions of the h th class of $1, 2, \dots, k$; A_k^h the sum without repetitions. If $0 < h < p-1$,

$$C_k^j \equiv 0 \pmod{p}, \quad j = p-k, \dots, p-2; \quad C_{np+k}^h \equiv C_k^h.$$

For $h = p-1$, $C_{np+k}^{p-1} \equiv n+1$ for $k=1, \dots, p$. For $h = m(p-1) + t$, $C_k^h \equiv C_k^t$ when $k < p+1$. For $1 < h < k$, the sum of C_k^h and A_k^h is divisible by $k^2(k+1)^2$; likewise, each C and A if h is odd. For $h < 2k$, $C_k^h - A_k^h$ is divisible by $2k+1$. The sum of the $2n$ th powers of $1, \dots, k$ is divisible by $2k+1$.

K. Hensel²⁰⁴ has given the further generalization: If $a_1, \dots, a_n, b_1, \dots, b_v$ are $n+v = p-1$ integers congruent modulo p to $1, 2, \dots, p-1$ in some order, and

$$\psi(x) = (x-b_1) \dots (x-b_v) = x^v - B_1 x^{v-1} + \dots \pm B_v,$$

then, for any j , $P_{nj} \equiv (-1)^{j_0} B_{j_0} \pmod{p}$, where j_0 is the least residue of j mod $p-1$ and $B_k = 0$ ($k > v$).

For Steiner's X_n , $X_n \psi(x) \equiv x^{p-1} - 1 \pmod{p}$. Multiply (1) by $x^n(x^{p-1}-1)$. Thus

$$\begin{aligned} x^n \psi(x) &\equiv x^{p-1} + P_{n1} x^{p-2} + \dots + P_{np-2} x + P_{np-1} - 1 + \frac{P_{np} - P_{n1}}{x} \\ &\quad + \frac{P_{np+1} - P_{n2}}{x^2} + \dots \pmod{p}. \end{aligned}$$

Replace $\psi(x)$ by its initial expression and compare coefficients. Hence

$$\begin{aligned} P_{ni+p-1} &\equiv P_{ni}, & P_{nv+1} &\equiv P_{nv+2} \equiv \dots \equiv P_{np-2} \equiv 0, & P_{np-1} &\equiv 1, \\ P_{nj} &\equiv (-1)^j B_j \quad (j=1, \dots, v). \end{aligned}$$

Taking $v = j = p-2$ and choosing $2, \dots, p-1$ for b_1, \dots, b_v , we get $1 \equiv -(p-1)! \pmod{p}$.

CONVERSE OF FERMAT'S THEOREM.

In a Chinese manuscript dating from the time of Confucius it is stated erroneously that $2^{n-1} - 1$ is not divisible by n if n is not prime (Jeans²²⁰).

Leibniz in September 1680 and December 1681 (Mahnke,⁷ 49-51) stated incorrectly that $2^n - 2$ is not divisible by n if n is not a prime. If $n = rs$, where r is the least prime factor of n , the binomial coefficient $\binom{n}{r}$ was shown to be not divisible by n , since $n-1, \dots, n-r+1$ are not divisible by r , whence not all the separate terms in the expansion of $(1+1)^n - 2$ are

²⁰³Ueber die Theilbarkeit der Combinationssummen aus den natürlichen Zahlen durch Primzahlen, Progr., Bremen, 1864, 20 pp.

²⁰⁴Archiv Math. Phys., (3), 1, 1901, 319; Kronecker's Zahlentheorie 1, 1901, 503.

divisible by n . From this fact Leibniz concluded erroneously that the expression itself is not divisible by n .

Chr. Goldbach²¹⁰ stated that $(a+b)^p - a^p - b^p$ is divisible by p also when p is any composite number. Euler (p. 124) points out the error by noting that $2^{35} - 2$ is divisible by neither 5 nor 7.

In 1769 J. H. Lambert¹⁵ (p. 112) proved that, if $d^m - 1$ is divisible by a , and $d^n - 1$ by b , where a, b are relatively prime, then $d^c - 1$ is divisible by ab if c is the l. c. m. of m, n (since divisible by $d^m - 1$ and hence by a). This was used to prove that if g is odd [and prime to 5] and if the decimal fraction for $1/g$ has a period of $g-1$ terms, then g is a prime. For, if $g = ab$ [where a, b are relatively prime integers > 1], $1/a$ has a period of m terms, $m \leq a-1$, and $1/b$ a period of n terms, $n \leq b-1$, so that the number of terms in the period for $1/g$ is $\leq (a-1)(b-1)/2 < g-1$. Thus Lambert knew at least the case $k = 10$ of the converse of Fermat's theorem (Lucas^{214, 217}).

An anonymous writer²¹¹ stated that $2n+1$ is or is not a prime according as one of the numbers $2^n \pm 1$ is or is not divisible by n . F. Sarrus²¹² noted the falsity of this assertion since $2^{170} - 1$ is divisible by the composite number 341.

In 1830 an anonymous writer⁴³ noted that $a^{n-1} - 1$ may be divisible by n when n is composite. In $a^{p-1} = kp + 1$, where p is a prime, set $k = \lambda q$. Then $a^{(p-1)q} \equiv 1 \pmod{pq}$. Thus $a^{pq-1} \equiv 1$ if $a^{q-1} \equiv 1 \pmod{pq}$, and the last will hold if $q-1$ is a multiple of $p-1$; for example, if $p = 11, q = 31, a = 2$, whence $2^{340} \equiv 1 \pmod{341}$.

V. Bouniakowsky²¹³ proved that if N is a product of two primes and if $N-1$ is divisible by the least positive integer a for which $2^a \equiv 1$, whence $2^{N-1} \equiv 1 \pmod{N}$, then each of the two primes decreased by unity is divisible by a . He noted that $3^6 \equiv 1 \pmod{91 = 7 \cdot 13}$.

E. Lucas²¹⁴ noted that $2^{n-1} \equiv 1 \pmod{n}$ for $n = 37 \cdot 73$ and stated the true converse to Fermat's theorem: If $a^x - 1$ is divisible by p for $x = p-1$, but not for $x < p-1$, then p is a prime.

F. Proth²¹⁵ stated that, when a is prime to n , n is a prime if $a^x \equiv 1 \pmod{n}$ for $x = (n-1)/2$, but for no other divisor of $(n-1)/2$; also, if $a^x \equiv 1 \pmod{n}$ for $x = n-1$, but for no divisor $< \sqrt{n}$ of $n-1$. If $n = m \cdot 2^k + 1$, where m is odd and $< 2^k$, and if a is a quadratic non-residue of n , then n is a prime if and only if $a^{(n-1)/2} \equiv -1 \pmod{n}$. If p is a prime $> \frac{1}{2}\sqrt{n}$, $n = mp + 1$ is a prime if $a^{n-1} - 1$ is divisible by n , but $a^m \not\equiv 1$ is not.

*F. Thaarup²¹⁶ showed how to use $a^{n-1} \equiv 1 \pmod{n}$ to tell if n is prime.

E. Lucas²¹⁷ proved the converse of Fermat's theorem: If $a^x \equiv 1 \pmod{n}$ for $x = n-1$, but not for x a proper divisor of $n-1$, then n is a prime.

²¹⁰Corresp. Math. Phys. (ed. Fuss), I, 1843, 122, letter to Euler, Apr. 12, 1742.

²¹¹Annales de Math. (ed. Gergonne), 9, 1818-9, 320.

²¹²*Ibid.*, 10, 1819-20, 184-7.

²¹³Mém. Ac. Sc. St. Pétersbourg (math.), (6), 2, 1841 (1839), 447-69; extract in Bulletin, 6, 97-8.

²¹⁴Assoc. franç. avanc. sc., 5, 1876, 61; 6, 1877, 161-2; Amer. Jour. Math., 1, 1878, 302.

²¹⁵Comptes Rendus Paris, 87, 1878, 926.

²¹⁶Nyt Tidsskr. for Mat., 2A, 1891, 49-52.

²¹⁷Théorie des nombres, 1891, 423, 441.

G. Levi¹¹⁴ was of the erroneous opinion that P is prime or composite according as it is or is not a divisor of $10^{P-1}-1$ [criticized by Cipolla,²²⁹ p. 142].

K. Zsigmondy²¹⁸ noted that, if q is a prime $\equiv 1$ or $3 \pmod{4}$, then $2q+1$ is a prime if and only if it divides $(2^q+1)/3$ or 2^q-1 , respectively; $4q+1$ is a prime if and only if it divides $(2^{2q}+1)/5$.

E. B. Escott²¹⁹ noted that Lucas'²¹⁴ condition is sufficient but not necessary.

J. H. Jeans²²⁰ noted that if p, q are distinct primes such that $2^p \equiv 2 \pmod{q}$, $2^q \equiv 2 \pmod{p}$, then $2^{pq} \equiv 2 \pmod{pq}$, and found this to be the case for $pq = 11 \cdot 31, 19 \cdot 73, 17 \cdot 257, 31 \cdot 151, 31 \cdot 331$. He ascribed to Kossett the result $2^{n-1} \equiv 1 \pmod{n}$ for $n = 645$.

A. Korselt²²¹ noted this case 645 and stated that $a^p \equiv a \pmod{p}$ if and only if p has no square factor and $p-1$ is divisible by the l. c. m. of p_1-1, \dots, p_n-1 , where p_1, \dots, p_n are the prime factors of p .

J. Franel²²² noted that $2^{pq} \equiv 2 \pmod{pq}$, where p, q are distinct primes, requires that $p-1$ and $q-1$ be divisible by the least integer a for which $2^a \equiv 1 \pmod{pq}$. [Cf. Bouniakowsky.²¹³]

L. Gegenbauer^{222a} noted that $2^{pq-1} \equiv 1 \pmod{pq}$ if $p = 2^r - 1 = \kappa p \tau + 1$ and $q = \kappa \tau + 1$ are primes, as for $p = 31, q = 11$.

T. Hayashi²²³ noted that $2^n - 2$ is divisible by $n = 11 \cdot 31$. If odd primes p and q can be found such that $2^p \equiv 2, 2^q \equiv 2 \pmod{pq}$, then $2^{pq} - 2$ is divisible by pq . This is the case if $p-1$ and $q-1$ have a common factor p' for which $2^{p'} \equiv 1 \pmod{pq}$, as for $p = 23, q = 89, p' = 11$.

Ph. Jolivald²²⁴ asked whether $2^{N-1} \equiv 1 \pmod{N}$ if $N = 2^p - 1$ and p is a prime, noting that this is true if $p = 11$, whence $N = 2047$, not a prime. E. Malo²²⁵ proved this as follows:

$$N-1 = 2(2^{p-1}-1) = 2pm, \quad 2^{N-1} = (2^p)^{2m} = (N+1)^{2m} \equiv 1 \pmod{N}.$$

G. Ricalde²²⁶ noted that a similar proof gives $a^{N-a+1} \equiv 1 \pmod{N}$ if $N = a^p - 1$, and a is not divisible by the prime p .

H. S. Vandiver²²⁷ proved the conditions of J. Franel²²² and noted that they are not satisfied if $a < 10$. Solutions for $a = 10$ and $a = 11$ are $pq = 11 \cdot 31$ and $23 \cdot 89$, respectively.

H. Schapira²²⁸ noted that the test for the primality of N that $a^a \equiv 1$

²¹⁸Monatshefte Math. Phys., 4, 1893, 79.

²¹⁹L'intermédiaire des math., 4, 1897, 270.

²²⁰Messenger Math., 27, 1897-8, 174.

²²¹L'intermédiaire des math., 6, 1899, 143.

²²²Ibid., p. 142.

^{222a}Monatshefte Math. Phys., 10, 1899, 373.

²²³Jour. of the Physics School in Tokio, 9, 1900, 143-4. Reprinted in Abhand. Geschichte Math. Wiss., 28, 1910, 25-26.

²²⁴L'intermédiaire des math., 9, 1902, 258.

²²⁵Ibid., 10, 1903, 88.

²²⁶Ibid., p. 186.

²²⁷Amer. Math. Monthly, 9, 1902, 34-36.

²²⁸Tehebychef's Theorie der Congruenzen, ed. 2, 1902, 306.

(mod N) for $q = N - 1$, but for no smaller q , is practical only if it be known that a small number a is a primitive root of N .

G. Arnoux^{228a} gave numerical instances of the converse of Fermat's theorem.

M. Cipolla²²⁹ stated that the theorem of Lucas²¹⁷ implies that, if p is a prime and $k = 2, 4, 6$, or 10 , then $kp + 1$ is a prime if and only if $2^{kp} \equiv 1 \pmod{kp + 1}$. He treated at length the problem to find a for which $a^{P-1} \equiv 1 \pmod{P}$, given a composite P ; and the problem to find P , given a . In particular, we may take P to be any odd factor of $(a^{2p} - 1)/(a^2 - 1)$ if p is an odd prime not dividing $a^2 - 1$. Again, $2^{P-1} \equiv 1 \pmod{P}$ for $P = F_m F_n \dots F_s$, $m > n > \dots > s$, if and only if $2^s > m$, where $F_s = 2^{2^s} + 1$ is a prime. If p and $q = 2p - 1$ are primes and a is any quadratic residue of q , then $a^{pq-1} \equiv 1 \pmod{pq}$; we may take $a = 3$ if $p = 4n + 3$; $a = 2$ if $p = 4n + 1$; both $a = 2$ and $a = 3$ if $p = 12k + 1$; etc.

E. B. Escott²³⁰ noted that $e^{n-1} \equiv 1 \pmod{n}$ if $e^a - 1$ contains two or more primes whose product n is $\equiv 1 \pmod{a}$, and gave a list of 54 such n 's.

A. Cunningham²³¹ noted the solutions $n = F_3 F_4 F_5 F_6 F_7$, $n = F_4 \dots F_{15}$, etc. [cf. Cipolla], and stated that there exist solutions in which n has more than 12 prime factors. One with 12 factors is here given by Escott.

T. Banachiewicz²³² verified that $2^N - 2$ is divisible by N for N composite and < 2000 only when N is

$$341 = 11 \cdot 31, \quad 561 = 3 \cdot 11 \cdot 17, \quad 1387 = 19 \cdot 73, \quad 1729 = 7 \cdot 13 \cdot 19, \quad 1905 = 3 \cdot 5 \cdot 127.$$

Since $2^N - 2$ is evidently divisible by N for every $N = F_k = 2^{2^k} + 1$, perhaps Fermat was thus led to his false conjecture that every F_k is a prime.

R. D. Carmichael²³³ proved that there are composite values of n (a product of three or more distinct odd primes) for which $e^{n-1} \equiv 1 \pmod{n}$ holds for every e prime to n .

J. C. Morehead²³⁴ and A. E. Western proved the converse of Fermat's theorem.

D. Mahnke⁷ (pp. 51-2) discussed Leibniz' converse of Fermat's theorem in the form that n is a prime if $x^{n-1} \equiv 1 \pmod{n}$ for all integers x prime to n and noted that this is false when n is the square or higher power of a prime or the product of two distinct primes, but is true for certain products of three or more primes, as $3 \cdot 11 \cdot 17$, $5 \cdot 13 \cdot 17$, $5 \cdot 17 \cdot 29$, $5 \cdot 29 \cdot 73$, $7 \cdot 13 \cdot 19$.

R. D. Carmichael²³⁵ used the result of Lucas¹¹⁰ to prove that $a^{P-1} \equiv 1 \pmod{P}$ holds for every a prime to P if and only if $P - 1$ is divisible by $\lambda(P)$. The latter condition requires that, if P is composite, it be a product of three or more distinct odd primes. There are found 14 products P of

^{228a}Assoc. franç., 32, 1903, II, 113-4.

²²⁹Annali di Mat., (3), 9, 1903-4, 138-160.

²³⁰Messenger Math., 36, 1907, 175-6; French transl., Sphinx-Oedipe, 1907-8, 146-8.

²³¹Math. Quest. Educat. Times, (2), 14, 1908, 22-23; 6, 1904, 26-7, 55-6.

²³²Spraw. Tow. Nauk, Warsaw, 2, 1909, 7-10.

²³³Bull. Amer. Math. Soc., 16, 1909-10, 237-8.

²³⁴Ibid., p. 2.

²³⁵Amer. Math. Monthly, 19, 1912, 22-7.

three primes, as well as $P = 13 \cdot 37 \cdot 73 \cdot 457$, for each of which the congruence holds for every a prime to P .

Welsch²³⁶ stated that if $k = 4n + 1$ is composite and < 1000 , $2^{k-1} \equiv 1 \pmod{k}$ only for $k = 561$ and 645 ; hence $n^n \equiv 1 \pmod{k}$ for these two k 's.

P. Bachmann²³⁷ proved that $x^{pq-1} \equiv 1 \pmod{pq}$ is never satisfied by all integers prime to pq if p and q are distinct odd primes [Carmichael²³⁵].

SYMMETRIC FUNCTIONS OF $1, 2, \dots, p-1$ MODULO p .

Report has been made above of the work on this topic by Lagrange,¹⁸ Lionnet,⁶¹ Tchebychef,⁷⁵ Sylvester,⁷⁸ Ottinger,⁹² Lucas,¹⁰³ Cahen,¹²⁵ Aubry,¹³⁷ Arévalo,¹⁵⁰ Schuh,¹⁵² Frattini,¹⁵³ Steiner,²⁰⁰ Jacobi,²⁰¹ Hensel.²⁰⁴

We shall denote $1^n + 2^n + \dots + (p-1)^n$ by s_n , and take p to be a prime. E. Waring²⁵⁰ wrote a, β, \dots for $1, 2, \dots, x$, and considered

$$s = a^a \beta^b \gamma^c \dots + a^b \beta^a \gamma^c \dots + a^a \beta^b \gamma^d \dots$$

If $t = a + b + c + \dots$ is odd and $< x$, and $x + 1$ is prime, s is divisible by $(x + 1)^2$. If $t < 2x$ and a, b, \dots are all even and prime to $2x + 1$, s is divisible by $2x + 1$.

V. Bouniakowsky²⁵¹ noted that s_m is divisible by p^2 , if $p > 2$ and m is odd and not $\equiv 1 \pmod{p-1}$; also if both $m \equiv 1 \pmod{p-1}$ and $m \equiv 0 \pmod{p}$.

C. von Staudt²⁵² proved that, if $S_n(x) = 1 + 2^n + \dots + x^n$,

$$\begin{aligned} S_n(ab) &\equiv b S_n(a) + na S_{n-1}(a) S_1(b-1) \pmod{a^2}, \\ 2S_{2n+1}(a) &\equiv (2n+1)a S_{2n}(a) \pmod{a^2}. \end{aligned}$$

If a, b, \dots, l are relatively prime in pairs,

$$\frac{S_n(ab \dots l)}{ab \dots l} - \frac{S_n(a)}{a} - \dots - \frac{S_n(l)}{l} = \text{integer}.$$

A. Cauchy²⁵³ proved that $1 + 1/2 + \dots + 1/(p-1) \equiv 0 \pmod{p}$.

G. Eisenstein²⁵⁴ noted that $s_m \equiv -1$ or $0 \pmod{p}$ according as m is or is not divisible by $p-1$. If m, n are positive integers $< p-1$,

$$\sum_{\sigma=1}^{p-2} \sigma^m (\sigma+1)^n \equiv 0 \text{ or } -\binom{n}{p-1-m} \pmod{p},$$

according as $m+n < \text{or} \geq p-1$.

L. Poincot²⁵⁵ noted that, when a takes the values $1, \dots, p-1$, then $(ax)^n$ has the same residues modulo p as a^n , order apart. By addition, $s_n x^n \equiv s_n \pmod{p}$. Take x to be one of the numbers not a root of $x^n \equiv 1$. Hence $s_n \equiv 0 \pmod{p}$ if n is not divisible by $p-1$.

²³⁶L'intermédiaire des math., 20, 1913, 94.

²³⁷Archiv Math. Phys., (3), 21, 1913, 185-7.

²⁵⁰Meditationes algebraicae, ed. 3, 1782, 382.

²⁵¹Bull. Ac. Sc. St. Pétersbourg, 4, 1838, 65-9.

²⁵²Jour. für Math., 21, 1840, 372-4.

²⁵³Mém. Ac. Sc. de l'Institut de France, 17, 1840, 340-1, footnote; Oeuvres, (1), 3, 81-2.

²⁵⁴Jour. für Math., 27, 1844, 292-3; 28, 1844, 232.

²⁵⁵Jour. de Math., 10, 1845, 33-4.

J. A. Serret²⁵⁶ concluded by applying Newton's identities to $(x-1)\dots(x-p+1)\equiv 0$ that $s_n\equiv 0 \pmod{p}$ unless n is divisible by $p-1$.

J. Wolstenholme²⁵⁷ proved that the numerators of

$$1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1}, \quad 1+\frac{1}{2^2}+\dots+\frac{1}{(p-1)^2}$$

are divisible by p^2 and p respectively, if p is a prime > 3 . Proofs have also been given by C. Leudesdorf²⁵⁸, A. Rieke,²⁵⁹ E. Allardice,²⁶⁰ G. Osborn,²⁶¹ L. Birkenmajer,²⁶² P. Niewenglowski,²⁶³ N. Nielsen,²⁶⁴ H. Valentiner,²⁶⁵ and others.²⁶⁶

V. A. Lebesgue²⁶⁷ proved that s_m is divisible by p if m is not divisible by $p-1$ by use of the identities

$$(n+1) \sum_{k=1}^x k(k+1)\dots(k+n-1) = x(x+1)\dots(x+n) \quad (n=1, \dots, p-1).$$

P. Frost²⁶⁸ proved that, if p is a prime not dividing $2^{2r}-1$, the numerators of σ_{2r} , σ_{2r-1} , $p(2r-1)\sigma_{2r}+2\sigma_{2r-1}$ are divisible by p , p^2 , p^3 , respectively, where

$$\sigma_k = 1 + \frac{1}{2^k} + \dots + \frac{1}{(p-1)^k}.$$

The numerator of the sum of the first half of the terms of σ_{2r} is divisible by p ; likewise that of the sum of the odd terms.

J. J. Sylvester²⁶⁹ stated that the sum $S_{n,m}$ of all products of n distinct numbers chosen from $1, \dots, m$ is the coefficient of t^n in the expansion of $(1+t)(1+2t)\dots(1+mt)$ and is divisible by each prime $> n+1$ contained in any term of the set $m-n+1, \dots, m, m+1$.

E. Fergola²⁷⁰ stated that, if $(a, b, \dots, l)^n$ represents the expression obtained from the expansion of $(a+b+\dots+l)^n$ by replacing each numerical coefficient by unity, then

$$(x, x+1, \dots, x+r)^n = \sum_{j=0}^n \binom{r+n}{j} (1, 2, \dots, r)^{n-j} x^j.$$

²⁵⁶Cours d'algèbre supérieure, ed. 2, 1854, 324.

²⁵⁷Quar. Jour. Math., 5, 1862, 35-39.

²⁵⁸Proc. London Math. Soc., 20, 1889, 207.

²⁵⁹Zeitschrift Math. Phys., 34, 1889, 190-1.

²⁶⁰Proc. Edinburgh Math. Soc., 8, 1890, 16-19.

²⁶¹Messenger Math., 22, 1892-3, 51-2; 23, 1893-4, 58.

²⁶²Prace Mat. Fiz., Warsaw, 7, 1896, 12-14 (Polish).

²⁶³Nouv. Ann. Math., (4), 5, 1905, 103.

²⁶⁴Nyt Tidsskrift for Mat., 21, B, 1909-10, 8-10.

²⁶⁵Ibid., p. 36-7.

²⁶⁶Math. Quest. Educat. Times, 48, 1888, 115; (2), 22, 1912, 99; Amer. Math. Monthly, 22, 1915, 103, 138, 170.

²⁶⁷Introd. à la théorie des nombres, 1862, 79-80, 17.

²⁶⁸Quar. Jour. Math., 7, 1866, 370-2.

²⁶⁹Giornale di Mat., 4, 1866, 344. Proof by Sharp, Math. Ques. Educ. Times, 47, 1887, 145-6; 63, 1895, 38.

²⁷⁰Ibid., 318-9. Cf. Wronski¹⁸¹ of Ch. VIII.

The number $(1, 2, \dots, r)^n$ is divisible by every prime $> r$ which occurs in the series $n+2, n+3, \dots, n+r$.

G. Torelli²⁷¹ proved that

$$\begin{aligned}(a_1, \dots, a_n)^r &= (a_1, \dots, a_{n-1})^r + a_n(a_1, \dots, a_n)^{r-1}, \\ (a_1, \dots, a_n, b)^r - (a_1, \dots, a_n, c)^r &= (b-c)(a_1, \dots, a_n, b, c)^{r-1}, \\ (x+a_0, x+a_1, \dots, x+a_n)^r &= \sum \binom{n+r}{j} (a_0, \dots, a_n)^{r-j} x^j,\end{aligned}$$

which becomes Fergola's for $a_i = i$ ($i=0, \dots, n$). Proof is given of Sylvester's²⁶⁹ theorem and the generalization that $S_{j,i}$ is divisible by $\binom{i+1}{j+1}$.

Torelli²⁷² proved that the sum $\sigma_{n,m}$ of all products of n equal or distinct numbers chosen from $1, 2, \dots, m$ is divisible by $\binom{n+m}{n+1}$, and gave recursion formulas for $\sigma_{n,m}$.

C. Sardi²⁷³ deduced Sylvester's theorem from the equations $A_1 = \binom{p}{2}, \dots$ used by Lagrange.¹⁸ Solving them for $A_p = S_{p,n}$, we get

$$p!(-1)^{p+1}S_{p,n} = \begin{vmatrix} -1 & 0 & 0 & \dots & 0 & \binom{n+1}{2} \\ \binom{n}{2} & -2 & 0 & \dots & 0 & \binom{n+1}{3} \\ \binom{n}{3} & \binom{n-1}{2} & -3 & \dots & 0 & \binom{n+1}{4} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \binom{n}{p} & \binom{n-1}{p-1} & \binom{n-2}{p-2} & \dots & \binom{n-p+2}{2} & \binom{n+1}{p+1} \end{vmatrix}.$$

If $n+1$ is a prime we see by the last column that $S_{n-1,n}$ is divisible by $n+1$. When $p=n-1$, denote the determinant by D . Then if $n+1$ is a prime, D is evidently divisible by $n+1$. Conversely, if D is divisible by $n+1$ and the quotient by $(n-1)!$, then $n+1$ is a prime. It is shown that

$$mS_{m,n} = \sum_{p=1}^m (-1)^{p+1} r_p S_{m-p,n}, \quad r_p = 1^p + \dots + n^p.$$

Using this for $m=1, \dots, n$, we see that r_p is divisible by any integer prime to $2, 3, \dots, p+1$ which occurs in $n+1$ or n . Hence if $n+1$ is a prime, it divides r_1, \dots, r_{n-1} , while $r_n \equiv n \pmod{n+1}$. If $n+1$ divides r_{n-1} it is a prime.

Sardi²⁷⁴ proved Sylvester's theorem and the formula

$$\sum_{r=0}^k (-1)^r S_{r, n+r-1} \sigma_{k-r, n+r} = 0,$$

stated by Fergola.²⁷⁵

²⁷¹Giornale di Mat., 5, 1867, 110-120.

²⁷²Ibid., 250-3.

²⁷³Ibid., 371-6.

²⁷⁴Ibid., 169-174.

²⁷⁵Ibid., 4, 1866, 380.

Sylvester²⁷⁶ stated that, if p_1, p_2, \dots are the successive primes 2, 3, 5, \dots ,

$$S_{j,n} = \frac{(n+1)n(n-1)\dots(n-j+1)}{p_1^{e_1} p_2^{e_2} \dots} F_{j-1}(n),$$

where $F_k(n)$ is a polynomial of degree k with integral coefficients, and the exponent e of the prime p is given by

$$e = \sum_{k=0}^{\infty} \left[\frac{j}{(p-1)p^k} \right].$$

E. Cesàro²⁷⁷ stated Sylvester's²⁶⁹ theorem and remarked that $S_{n,m} - n!$ is divisible by $m - n$ if $m - n$ is a prime.

E. Cesàro²⁷⁸ stated that the prime p divides $S_{m,p-2} - 1$, $S_{p-1,p} + 1$, and, except when $m = p - 1$, $S_{m,p-1}$. Also (p. 401), each prime $p > (n+1)/2$ divides $S_{p-1,n} + 1$, while a prime $p = (n+1)/2$ or $n/2$ divides $S_{p-1,n} + 2$.

O. H. Mitchell²⁷⁹ discussed the residues modulo k (any integer) of the symmetric functions of $0, 1, \dots, k-1$. To this end he evaluated the residue of $(x-a)(x-\beta)\dots$, where α, β, \dots are the s -totitives of k (numbers $< k$ which contain s but no prime factor of k not found in s). The results are extended to the case of moduli $p, f(x)$, where p is a prime [see Ch. VIII].

F. J. E. Lionnet²⁸⁰ stated and Moret-Blanc proved that, if $p = 2n+1$ is a prime > 3 , the sum of the powers with exponent $2a$ (between zero and $2n$) of $1, 2, \dots, n$, and the like sum for $n+1, n+2, \dots, 2n$, are divisible by p .

M. d'Ocagne²⁸¹ proved the first relation of Torelli.²⁷¹

E. Catalan²⁸² stated and later proved²⁸³ that s_k is divisible by the prime $p > k+1$. If p is an odd prime and $p-1$ does not divide k , s_k is divisible by p ; while if $p-1$ divides k , $s_k \equiv -1 \pmod{p}$. Let $p = a^a b^b \dots$; if no one of $a-1, b-1, \dots$ divides k , s_k is divisible by p ; in the contrary case, not divisible. If p is a prime > 2 , and $p-1$ is not a divisor of $k+l$, then

$$S = 1^k(p-1)^l + 2^k(p-2)^l + \dots + (p-1)^{k1^l}$$

is divisible by p ; but, if $p-1$ divides $k+l$, $S \equiv -(-1)^l \pmod{p}$. If k and l are of contrary parity, p divides S .

M. d'Ocagne²⁸⁴ proved for Fergola's²⁷⁰ symbol the relation

$$(a \dots fg \dots l \dots v \dots z)^n = \sum (a \dots f)^\lambda (g \dots l)^\mu \dots (v \dots z)^\rho,$$

summed for all combinations such that $\lambda + \mu + \dots + \rho = n$. Denoting by $a^{(p)}$ the letter a taken p times, we have

$$(a^{(p)} ab \dots l)^n = \sum_{i=0}^n a^{i(1^{(p)})^i} (ab \dots l)^{n-i}.$$

²⁷⁶Nouv. Ann. Math., (2), 6, 1867, 48.

²⁷⁷Nouv. Corresp. Math., 4, 1878, 401; Nouv. Ann. Math., (3), 2, 1883, 240.

²⁷⁸Nouv. Corresp. Math., 4, 1878, 368.

²⁷⁹Amer. Jour. Math., 4, 1881, 25-38.

²⁸⁰Nouv. Ann. Math., (3), 2, 1883, 384; 3, 1884, 395-6.

²⁸¹Ibid., (3), 2, 1883, 220-6. Cf. Cesàro, (3), 4, 1885, 67-9.

²⁸²Bull. Ac. Sc. Belgique, (3), 7, 1884, 448-9.

²⁸³Mém. Ac. R. Sc. Belgique, 46, 1886, No. 1, 16 pp.

²⁸⁴Nouv. Ann. Math., (3), 5, 1886, 257-272.

It is shown that $(1^{(p)})^n$ equals the number of combinations of $n+p-1$ things $p-1$ at a time. Various algebraic relations between binomial coefficients are derived.

L. Gegenbauer²⁸⁵ considered the polynomial

$$f(x) = \sum_{i=0}^{p-2+k} b_i x^i \quad (1-p < k \leq p-1)$$

and proved that

$$\sum_{\lambda=1}^{p-1} f(\lambda)/\lambda^{p-2} \equiv -b_{p-2} \pmod{p}, \quad k < p-1,$$

$$\sum_{\lambda=1}^{p-1} f(\lambda)/\lambda^{p-1} \equiv -b_{p-2} - b_{2p-3} \pmod{p}, \quad k = p-1,$$

and deduced the theorem on the divisibility of s_n by p .

E. Lucas²⁸⁶ proved the theorem on the divisibility of s_n by p by use of the symbolic expression $(s+1)^n - s^n$ for $x^n - 1$.

N. Nielsen^{286a} proved that if p is an odd prime and if k is odd and $1 < k < p-1$, the sum of the products of $1, \dots, p-1$ taken k at a time is divisible by p^2 . For $k=p-2$ this result is due to Wolstenholme.²⁸⁷

N. M. Ferrers²⁸⁷ proved that, if $2n+1$ is a prime, the sum of the products of $1, 2, \dots, 2n$ taken r at a time is divisible by $2n+1$ if $r < 2n$ [Lagrange¹⁸], while the sum of the products of the squares of $1, \dots, n$ taken r at a time is divisible by $2n+1$ if $r < n$. [Other proofs by Glaisher.²⁹⁴]

J. Perott²⁸⁸ gave a new proof that s_n is divisible by p if $n < p-1$.

R. Rawson²⁸⁹ proved the second theorem of Ferrers.

G. Osborn²⁹⁰ proved for $r < p-1$ that s_r is divisible by p if r is even, by p^2 if r is odd; while the sum of the products of $1, \dots, p-1$ taken r at a time is divisible by p^2 if r is odd and $1 < r < p$.

J. W. L. Glaisher²⁹¹ stated theorems on the sum $S_r(a_1, \dots, a_i)$ of the products of a_1, \dots, a_i taken r at a time. If r is odd, $S_r(1, \dots, n)$ is divisible by $n+1$ (special case $n+1$ a prime proved by Lagrange and Ferrers). If r is odd and > 1 , and if $n+1$ is a prime > 3 , $S_r(1, \dots, n)$ is divisible by $(n+1)^2$ [Nielsen^{286a}]. If r is odd and > 1 , and if n is a prime > 2 , $S_r(1, \dots, n)$ is divisible by n^2 . If $n+1$ is a prime, $S_r(1^2, \dots, n^2)$ is divisible by $n+1$ for $r=1, \dots, n-1$, except for $r=n/2$, when it is congruent to $(-1)^{1+n/2}$ modulo $n+1$. If p is a prime $\leq n$, and k is the quotient obtained on dividing $n+1$ by p , then $S_{p-1}(1, \dots, n) \equiv -k \pmod{p}$; the case $n=p-1$ is Wilson's theorem.

²⁸⁵Sitzungsber. Ak. Wiss. Wien (Math.), 95 II, 1887, 616-7.

²⁸⁶Théorie des nombres, 1891, 437.

^{286a}Nyt Tidsskrift for Mat., 4, B, 1893, 1-10.

²⁸⁷Messenger Math., 23, 1893-4, 56-58.

²⁸⁸Bull. des sc. math., 18, I, 1894, 64. Other proofs, Math. Quest. Educ. Times, 58, 1893, 109; 4, 1903, 42.

²⁸⁹Messenger Math., 24, 1894-5, 68-69.

²⁹⁰Ibid., 25, 1895-6, 68-69.

²⁹¹Ibid., 28, 1898-9, 184-6. Proofs²⁹⁴.

S. Monteiro²⁹² noted that $2n+1$ divides $(2n)! \Sigma_1^{2n} 1/r$.

J. Westlund²⁹³ reproduced the discussion by Serret²⁵⁶ and Tchebychef.⁷⁵

Glaisher²⁹⁴ proved his²⁹¹ earlier theorems. Also, if $p=2m+1$ is prime,

$$(m-t)pS_{2t}(1, \dots, 2m) \equiv S_{2t+1}(1, \dots, 2m) \pmod{p^3}$$

and, if $t > 1$, modulo p^4 . According as n is odd or even,

$$S_{2t}(1, \dots, n) \equiv S_{2t}(1, \dots, n-1) \pmod{n^2 \text{ or } \frac{1}{2}n^2}.$$

For m odd and > 3 , $S_{2m-3}(1, \dots, 2m-1)$ is divisible by m^2 , and

$$S_{m-2}(1^2, \dots, \{m-1\}^2), \quad S_{2m-4}(1, \dots, 2m-1)$$

are divisible by m . He gave the values of $S_r(1, \dots, n)$ and $A_r = S_r(1, \dots, n-1)$ in terms of n for $r=1, \dots, 7$; the numerical values of $S_r(1, \dots, n)$ for $n \leq 22$, and a list of known theorems on the divisors of A_r and S_r . For r odd, $3 \leq r \leq m-2$, $S_r(1, \dots, 2m-1)$ is divisible by m and, if m is a prime > 3 , by m^2 . He proved (*ibid.*, p. 321) that, if $1 \leq r \leq (p-3)/2$, and B_r is a Bernoulli number,

$$\frac{2S_{2r+1}(1, \dots, p-1)}{p^2} \equiv \frac{-(2r+1)S_{2r}(1, \dots, p-1)}{p},$$

$$\frac{S_{2r}(1, \dots, p-1)}{p} \equiv \frac{(-1)^r B_r}{2r} \pmod{p}.$$

Glaisher²⁹⁵ gave the residues of σ_k [Frost²⁶⁸] modulo p^2 and p^3 and proved that $\sigma_2, \sigma_4, \dots, \sigma_{p-3}$ are divisible by p , and $\sigma_3, \sigma_5, \dots, \sigma_{p-2}$ by p^2 , if p is a prime.

Glaisher²⁹⁶ proved that, if p is an odd prime,

$$1 + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \dots + \frac{1}{(p-2)^{2n}} \equiv 0 \text{ or } -\frac{1}{2} \pmod{p},$$

according as $2n$ is not or is a multiple of $p-1$. He obtained (pp. 154-162) the residue of the sum of the inverses of like powers of numbers in arithmetical progression.

F. Sibirani^{296a} proved for the $S_{n,m}$ of Sylvester²⁶⁹ (designated $s_{n,m+1}$) that

$$S_{i,j} = jS_{i-1,j-1} + S_{i,j-1},$$

$$\begin{vmatrix} S_{n,n} & S_{n-1,n} & \dots & S_{n-k+1,n} \\ \dots & \dots & \dots & \dots \\ S_{n+k-1,n+k-1} & S_{n+k-2,n+k-1} & \dots & S_{n,n+k-1} \end{vmatrix} = (n!)^k.$$

²⁹²Jornal Sc. Mat. Phys. e Nat., Lisbon, 5, 1898, 224.

²⁹³Proc. Indiana Ac. Sc., 1900, 103-4.

²⁹⁴Quar. Jour. Math., 31, 1900, 1-35.

²⁹⁵*Ibid.*, 329-39; 32, 1901, 271-305.

²⁹⁶Messenger Math., 30, 1900-1, 26-31.

^{296a}Periodico di Mat., 16, 1900-1, 279-284.

K. Hensel²⁹⁷ proved by the method of Poinso²⁵⁵ that any integral symmetric function of degree v of $1, \dots, p-1$ with integral coefficients is divisible by the prime p if v is not a multiple of $p-1$.

W. F. Meyer²⁹⁸ gave the generalization that, if a_1, \dots, a_{p-1} are incongruent modulo p^n , and each $a_i^{p-1} - 1$ is divisible by p^n , any integral symmetric function of degree v of a_1, \dots, a_{p-1} is divisible by p^n if v is not a multiple of $p-1$. Of the $\phi(p^n)$ residues modulo p^n , prime to p , there are $p^k(p-1)^2$ for which $a^{p-1} - 1$ is divisible by p^{n-1-k} , but by no higher power of p , where $k=1, \dots, n-1$; the remaining $p-1$ residues give the above a_1, \dots, a_{p-1} .

J. W. Nicholson²⁹⁹ noted that, if p is a prime, the sum of the n th powers of p numbers in arithmetical progression is divisible by p if $n < p-1$, and $\equiv -1 \pmod{p}$ if $n = p-1$.

G. Wertheim³⁰⁰ proved the same result by use of a primitive root.

A. Aubry³⁰¹ took $x=1, 2, \dots, p-1$ in

$$(x+1)^n - x^n = nx^{n-1} + Ax^{n-2} + \dots + Lx + 1$$

and added the results. Thus

$$p^n = ns_{n-1} + As_{n-2} + \dots + Ls_1 + p.$$

Hence by induction s_{n-1} is divisible by the prime p if $n < p$. He attributed this theorem to Gauss and Libri without references.

U. Concina³⁰² proved that s_n is divisible by the prime $p > 2$ if n is not divisible by $p-1$. Let δ be the g. c. d. of $n, p-1$, and set $\mu\delta = p-1$. The μ distinct residues r_i of n th powers modulo p are the roots of $x^\mu \equiv 1 \pmod{p}$, whence $\sum r_i \equiv 0 \pmod{p}$ for n not divisible by $p-1$. For each r_i , $x^n \equiv r_i$ has δ incongruent roots. Hence $s_n \equiv \delta \sum r_i \equiv 0$. He proved also that, if $p+1$ is a prime > 3 , and n is even and not divisible by p , $1^n + 2^n + \dots + (p/2)^n$ is divisible by $p+1$.

W. H. L. Janssen van Raay³⁰³ considered, for a prime $p > 3$,

$$A_h = \frac{(p-1)!}{h}, \quad B_h = \frac{(p-1)!}{h(p-h)}$$

and proved that $B_1 + B_2 + \dots + B_{(p-1)/2}$ is divisible by p , and

$$A_1 + \dots + A_{p-1}, \quad 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$$

are divisible by p^2 .

U. Concina³⁰⁴ proved that $S = 1 + 2^n + \dots + k^n$ is divisible by the odd number k if n is not divisible by $p-1$ for any prime divisor of p of k . Next, let k be even. For n odd > 1 , S is divisible by k or only by $k/2$ according

²⁹⁷Archiv Math. Phys., (3), 1, 1901, 319. Inserted by Hensel in Kronecker's Vorlesungen über Zahlentheorie I, 1901, 104-5, 504.

²⁹⁸Archiv Math. Phys., (3), 2, 1902, 141. Cf. Meissner³⁹ of Ch. IV.

²⁹⁹Amer. Math. Monthly, 9, 1902, 212-3. Stated, 1, 1894, 188.

³⁰⁰Anfangsgründe der Zahlentheorie, 1902, 265-6.

³⁰¹L'enseignement math., 9, 1907, 296.

³⁰²Periodico di Mat., 27, 1912, 79-83.

³⁰³Nieuw Archief voor Wiskunde, (2), 10, 1912, 172-7.

³⁰⁴Periodico di Mat., 28, 1913, 164-177, 267-270.

as k is or is not divisible by 4. For n even, S is divisible only by $k/2$ provided n is not divisible by any prime factor, diminished by unity, of k .

N. Nielsen³⁰⁵ wrote C_p^r for the sum of the products r at a time of $1, \dots, p-1$, and

$$s_n(p) = \sum_{s=1}^p s^n, \quad \sigma_n(p) = \sum_{s=1}^p (-1)^{p-s} s^n.$$

If p is a prime $> 2n+1$,

$$\sigma_{2n}(p-1) \equiv s_{2n}(p-1) \equiv 0 \pmod{p}, \quad s_{2n+1}(p-1) \equiv 0 \pmod{p^2}.$$

If $p = 2n+1$ is a prime > 3 , and $1 \leq r \leq n-1$, C_p^{2r+1} is divisible by p^2 .

Nielsen³⁰⁶ proved that $2D_n^{2p+1}$ is divisible by $2n$ for $2p+1 \leq n$, where D_n^* is the sum of the products of $1, 3, 5, \dots, 2n-1$ taken s at a time; also,

$$2^{2q+1} s_{2q}(n-1) \equiv 2^{2q} s_{2q}(2n-1) \pmod{4n^2},$$

and analogous congruences between sums of powers of successive even or successive odd integers, also when alternate terms are negative. He proved (pp. 258-260) relations between the C 's, including the final formulas by Glaisher.²⁹⁴

Nielsen³⁰⁷ proved the results last cited. Let p be an odd prime. If $2n$ is not divisible by $p-1$, $s_{2n}(p-1) \equiv 0 \pmod{p}$, $s_{2n+1}(p-1) \equiv 0 \pmod{p^2}$. But if $2n$ is divisible by $p-1$,

$$s_{2n}(p-1) \equiv -1, \quad s_{2n+1}(p-1) \equiv 0 \pmod{p}, \quad s_p(p-1) \equiv 0 \pmod{p^2}.$$

T. E. Mason³⁰⁸ proved that, if p is an odd prime and i an odd integer > 1 , the sum A_i of the products i at a time of $1, \dots, p-1$ is divisible by p^2 . If p is a prime > 3 , s_k is divisible by p^2 when k is odd and not of the form $m(p-1)+1$, by p when k is even and not of the form $m(p-1)$, and not by p if k is of the latter form. If $k = m(p-1)+1$, s_k is divisible by p^2 or p according as k is or is not divisible by p . Let p be composite and r its least prime factor; then $r-1$ is the least integer t for which A_t is not divisible by p and conversely. Hence p is a prime if and only if $p-1$ is the least t for which A_t is not divisible by p . The last two theorems hold also if we replace A 's by s 's.

T. M. Putnam³⁰⁹ proved Glaisher's²⁹⁵ theorem that s_{-n} is divisible by p if n is not a multiple of $p-1$, and

$$\sum_{j=1}^{(p-1)/2} j^{p-2} \equiv \frac{2-2^p}{p} \pmod{p}.$$

W. Meissner³¹⁰ arranged the residues modulo p , a prime, of the successive

³⁰⁵K. Danske Vidensk. Selsk. Skrifter, (7), 10, 1913, 353.

³⁰⁶Annali di Mat., (3), 22, 1914, 81-94.

³⁰⁷Ann. sc. l'école norm. sup., (3), 31, 1914, 165, 196-7.

³⁰⁸Tôhoku Math. Jour., 5, 1914, 136-141.

³⁰⁹Amer. Math. Monthly, 21, 1914, 220-2.

³¹⁰Mitt. Math. Gesell. Hamburg, 5, 1915, 159-182.

powers of a primitive root h of p in a rectangular table of t rows and τ columns, where $t\tau = p-1$. For $p=13$, $h=2$, $t=4$, the table is shown here. Let R range over the numbers in any column. Then ΣR and $\Sigma 1/R$ are divisible by p . If t is even, $\Sigma 1/R$ is divisible by p^2 , as $1/1+1/8+1/12+1/5 = 13^2/120$. For $t=p-1$, the theorem becomes the first one due to Wolstenholme.²⁵⁷ Generalizations are given at the end of the paper.

N. Nielsen³¹¹ proved his^{286a} theorem and the final results of Glaisher.²⁹⁴ Nielsen³¹² proceeded as had Aubry³⁰¹ and then proved

$$s_{2n+1} \equiv 0 \pmod{p^2}, \quad \sum_{j=1}^{(p-1)/2} j^{2n} \equiv 0 \pmod{p}, \quad 1 \leq n \leq \frac{p-3}{2}.$$

Then by Newton's identities we get Wilson's theorem and Nielsen's³⁰⁵ last result.

E. Cahen³¹³ stated Nielsen's^{286a} theorem.

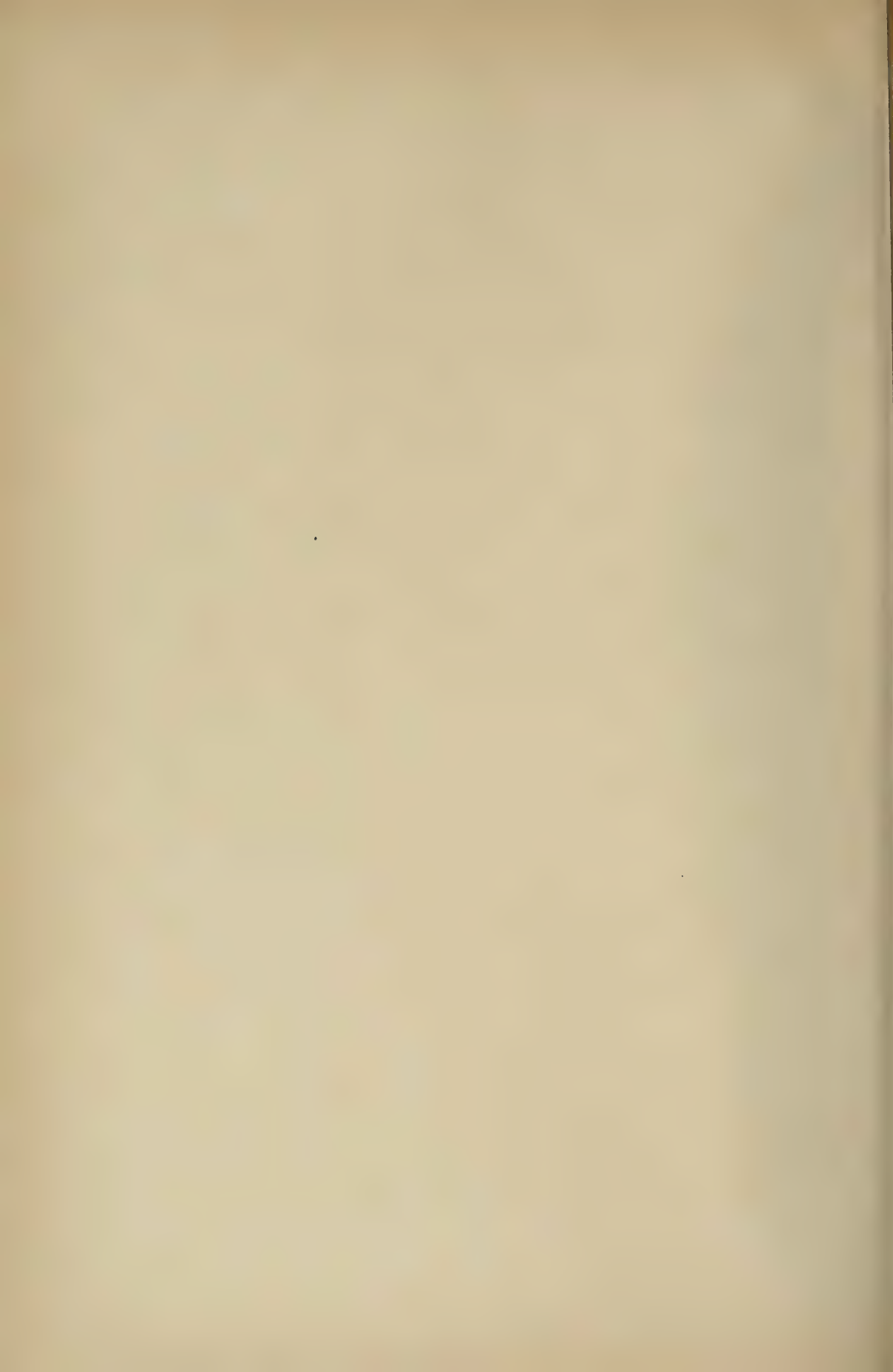
F. Irwin stated and E. B. Escott³¹⁴ proved that if S_j is the sum of the products j at a time of $1, 1/2, 1/3, \dots, 1/t$, where $t = (p-1)/2$, then $2S_2 - S_1^2$, etc., are divisible by the odd prime p .

³¹¹Oversigt Danske Vidensk. Selsk. Forhandling, 1915, 171-180, 521.

³¹²*Ibid.*, 1916, 194-5.

³¹³Comptes Rendus Séances Soc. Math. France, 1916, 29.

³¹⁴Amer. Math. Monthly, 24, 1917, 471-2.



CHAPTER IV.

RESIDUE OF $(U^{p-1}-1)/P$ MODULO P .

N. H. Abel¹ asked if there are primes p and integers a for which

$$(1) \quad a^{p-1} \equiv 1 \pmod{p^2}, \quad 1 < a < p.$$

C. G. J. Jacobi² noted that, for $p \leq 37$, (1) holds only when $p=11$, $a=3$ or 9 ; $p=29$, $a=14$; $p=37$, $a=18$. Cf. Thibault³¹ of Ch. VI.

G. Eisenstein³ noted that, for p a prime, the function

$$q_u = (u^{p-1} - 1)/p$$

has the properties

$$(2) \quad q_{uv} \equiv q_u + q_v, \quad q_{u+pv} \equiv q_u - \frac{v}{u} \pmod{p},$$

$$2q_2 \equiv 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots - \frac{1}{p-1} \equiv \sum_s \frac{1}{s} \pmod{p},$$

where $s = (p+1)/2, \dots, p-1$. All solutions of (1) are included in $a \equiv u + puq_u$, $0 < u < p$.

E. Desmarest⁴ noted that (1) holds for $p=487$, $a=10$, and stated that $p=3$ and $p=487$ are the only primes < 1000 for which 10 is a solution.

J. J. Sylvester⁵ stated that, if p, r are distinct primes, $p > 2$, then q_r is congruent modulo p to a sum of fractions with the successive denominators $p-1, \dots, 2, 1$ and (as corrected) with numerators the repeated cycle of the positive integers $\leq r$ congruent modulo r to $1/p, 2/p, \dots, r/p$. Thus, for $r=5$,

$$q_5 \equiv \frac{1}{p-1} + \frac{2}{p-2} + \frac{3}{p-3} + \frac{4}{p-4} + \frac{5}{p-5} + \frac{1}{p-6} + \dots \quad (p=10k+1),$$

$$q_5 \equiv \frac{3}{p-1} + \frac{1}{p-2} + \frac{4}{p-3} + \frac{2}{p-4} + \frac{5}{p-5} + \frac{3}{p-6} + \dots \quad (p=10k+7).$$

According as $p=4k+1$ or $4k-1$, q_2 is congruent to

$$\begin{aligned} & \frac{2}{p-3} + \frac{2}{p-4} + \frac{2}{p-7} + \frac{2}{p-8} + \frac{2}{p-11} + \dots, \\ & -\frac{2}{p-2} - \frac{2}{p-3} - \frac{2}{p-6} - \frac{2}{p-7} - \frac{2}{p-10} - \dots \end{aligned}$$

[the signs were given + erroneously]. For any p ,

$$q_2 \equiv -\frac{1}{p-1} + \frac{1}{p-2} - \frac{1}{p-3} + \dots \pmod{p}.$$

¹Jour. für Math., 3, 1828, 212; Oeuvres, 1, 1881, 619.

²Ibid., 301-2; Werke, 6, 238-9; Canon Arithmeticus, Berlin, 1839, Introd., xxxiv.

³Berlin Berichte, 1850, 41.

⁴Théorie des nombres, 1852, 295.

⁵Comptes Rendus Paris, 52, 1861, 161, 212, 307, 817; Phil. Mag., 21, 1861, 136; Coll. Math. Papers, II, 229-235, 241, 262-3.

Jean Plana⁶ developed $\{(M-1)+1\}^p$ and obtained

$$M^p - M - \{(M-1)^p - (M-1)\} = pf(M),$$

$$f(M) = M - 1 + \frac{p-1}{2}(M-1)^2 + \frac{(p-1)(p-2)}{2 \cdot 3}(M-1)^3 + \dots + (M-1)^{p-1}.$$

Take $M = m, m-1, \dots, 1$ in the first equation and add. Thus

$$\frac{m^p - m}{p} = f(1) + \dots + f(m) = s_1 + \frac{p-1}{2}s_2 + \dots + s_{p-1},$$

where $s_i = 1^i + 2^i + \dots + (m-1)^i$. For $j > 1$, we may replace p by j and get

$$m^j - m = js_{j-1} + \binom{j}{2}s_{j-2} + \binom{j}{3}s_{j-3} + \dots + js_1,$$

a result obtained by Plana by a long discussion [Euler⁴¹]. He concluded erroneously that each s_i is divisible by m (for $m=3, s_2=5$).

F. Proth⁷ stated that, if p is a prime, $2^p - 2$ is not divisible by p^2 [error, see Meissner³³].

M. A. Stern⁸ proved that, if p is an odd prime,

$$\begin{aligned} \frac{m^p - m}{p} &\equiv s_1 - \frac{1}{2}s_2 + \frac{1}{3}s_3 - \dots - \frac{1}{p-1}s_{p-1} \equiv \sigma_{p-1} + \frac{1}{2}\sigma_{p-2} + \dots + \frac{1}{p-1}\sigma_1 \\ &\equiv \frac{1}{2} \left(\frac{m}{p-1} + \frac{m^2}{p-2} + \dots + m^{p-1} \right) + \frac{1}{p-2}s_2 + \frac{1}{p-4}s_4 + \dots + s_{p-1} \pmod{p}, \end{aligned}$$

for s_i as by Plana and $\sigma_i = 1^i + 2^i + \dots + m^i$. Proof is given of the formula below (2) of Eisenstein³ and Sylvester's formulæ for q_2 (corrected), as well as several related formulæ.

L. Gegenbauer⁹ used Stern's congruences to prove that the coefficient of the highest power of x in a polynomial $f(x)$ of degree $p-2$ is congruent to $(m^p - m)/p$ modulo p if $f(x)$ satisfies one of the systems of equations

$$f(\lambda) = (-1)^{\lambda+1} \lambda^{p-3} s_\lambda(m-1), \quad f(\lambda) = \lambda^{p-3} s_{p-\lambda}(m) \quad (\lambda = 1, \dots, p-1).$$

E. Lucas¹⁰ proved that q_2 is a square only for $p=2, 3, 7$, and stated the result by Desmarest.⁴

F. Panizza¹¹ enumerated the combinations p at a time of ap distinct things separated into p sets of a each, by counting for each r the combinations of the things belonging to r of the p sets:

$$\binom{ap}{p} = \sum_{r=1}^p \binom{p}{r} \Sigma \binom{a}{i_1} \binom{a}{i_2} \dots \binom{a}{i_r},$$

⁶Mem. Acad. Turin, (2), 20, 1863, 120.

⁷Comptes Rendus Paris, 83, 1876, 1288.

⁸Jour. für Math., 100, 1887, 182-8.

⁹Sitzungsber. Ak. Wiss. Wien (Math.), 95, 1887, II, 616-7.

¹⁰Théorie des nombres, 1891, 423.

¹¹Periodico di Mat., 10, 1895, 14-16, 54-58.

where $i_1 + \dots + i_r = p$, $i_i > 0$. The term given by $r=p$ is a^p . For p a prime, the left member is $\equiv a \pmod{p}$ and we have Fermat's theorem. By induction on r ,

$$\Sigma \binom{a}{i_1} \dots \binom{a}{i_r} = \Sigma_{i=0}^{r-1} (-1)^i \binom{r}{i} \binom{(r-i)a}{p}.$$

Taking $r=p$, we have

$$\frac{a^p - a}{p} = \frac{1}{p} \left\{ \binom{ap}{p} - a \right\} + \Sigma_{i=1}^{p-1} (-1)^i \frac{1}{i} \binom{p-1}{i-1} \binom{(p-i)a}{p}.$$

D. Mirimanoff¹² wrote a_0 for the least positive integer making $a_0 p + 1$ divisible by the prime $r < p$, and denoted the quotient by $r^{e_0} b_1$, where b_1 is prime to r . Similarly, let a_i be the least positive integer such that $a_i p + b_i = r^{e_i} b_{i+1}$. We ultimately find an n for which $b_n = 1$. Then $b_{n+i} = b_i$. By (2),

$$q_{b_i} - \frac{a_i}{b_i} \equiv e_i q_r + q_{b_{i+1}}, \quad - \Sigma_{i=0}^{n-1} \frac{a_i}{b_i} \equiv q_r \Sigma e_i \pmod{p}.$$

Let r belong to the exponent ω modulo p and set $e\omega = p-1$. Then $\Sigma e_i = \omega$, while $1, b_1, \dots, b_{n-1}$ are the distinct residues of the e th powers of the integers $< r$ and prime to r . Thus

$$q_r \equiv e \Sigma_{i=0}^{n-1} \frac{a_i}{b_i} \pmod{p}.$$

The formula obtained by taking r a primitive root of p is included in the following, which holds also for any prime r :

$$q_r \equiv \Sigma_{\beta_i=1}^{p-1} \frac{a_i}{\beta_i} \pmod{p},$$

a_i being the least positive integer for which $a_i p + \beta_i \equiv 0 \pmod{r}$. Set $\beta_i = p - \delta$, $p'p \equiv 1 \pmod{r}$, $0 < p' < r$. Then $a_i \equiv p'\delta - 1 \pmod{r}$,

$$q_r \equiv \Sigma_{i=1}^{p-1} \frac{\{p'\delta\}}{p-\delta} \pmod{p},$$

$\{k\}$ being the least positive residue modulo r of k . Whence Sylvester's⁵ statement.

J. S. Aladow¹³ proved that (1) has at most $(p-1)/4$ roots if $p=4m \pm 1$.

A. Cunningham^{13a} listed 27 cases in which $r^{p-1} \equiv 1$ or $r^l \equiv 1 \pmod{p'}$, $r < p'^{l-1}$, where l is a divisor of $p-1$. For the 11 cases of the first kind, $p=5, 7, 17, 19, 29, 37, 43, 71, 487$.

W. Fr. Meyer¹⁴ proved by induction that, if p is a prime, $x^{p-1} - 1$ is divisible by p^k ($1 \leq k < n$), but not by p^{k+1} , for exactly $p^{n-1-k} (p-1)^2$ positive integers $x < p^n$ and prime to p , and is divisible by p^n for the remaining $p-1$ such integers. Set

$$A = a + \mu_1 p + \dots + \mu_n p^n \quad (1 \leq a < p, 0 \leq \mu_i < p), \quad \lambda_p = (a^{p^0} - a^{p^0-1})/p^0.$$

¹²Jour. für Math., 115, 1895, 295-300.

¹³St. Petersburg Math. Soc. (Russian), 1899, 40-44.

^{13a}Messenger Math., 29, 1899-1900, 158. See Cunningham^{12b}, Ch. VI.

¹⁴Archiv Math. Phys., (3), 2, 1901, 141-6.

If k is the least index for which $\mu_k \not\equiv \lambda_k$, $\mu_h \equiv \lambda_h \pmod{p}$ for $h < k$, then $A^{p-1} - 1$ is divisible by p^k , but not by p^{1+k} .

A. Palmström and A. Pollak¹⁵ proved that, if p is a prime and n, m are the exponents to which a belongs modulo p, p^2 , respectively, then $a^{np} - 1$ is divisible by p^2 , so that m is a multiple of n and a divisor of np , whence $m = n$ or pn . Thus according as a^{p-1} is or is not $\equiv 1 \pmod{p^2}$, $m = n$ or $m = np$.

Worms de Romilly^{15a} noted that, if ω is a primitive root of p^2 , the incongruent roots of $x^{p-1} \equiv 1 \pmod{p^2}$ are $\omega^{jp} (j = 1, \dots, p-1)$.

J. W. L. Glaisher¹⁶ proved that if r is a positive integer $< p$, p a prime,

$$r^{p-1} = 1 + g_1 p + \frac{1}{2}(g_1^2 - g_2)p^2 + \frac{1}{6}(g_1^3 - 3g_1 g_2 + 2g_3)p^3 + \dots,$$

where g_n is the sum of the n th powers of

$$\frac{1}{\sigma}, \frac{2}{[2\sigma]}, \dots, \frac{r-1}{[(r-1)\sigma]}, \frac{1}{r+\sigma}, \frac{2}{r+[2\sigma]}, \dots, \frac{r-1}{r+[(r-1)\sigma]}, \frac{1}{2r+\sigma}, \dots,$$

σ being the least positive residue modulo r of $-p$. If μ_i is the least positive solution of $\sigma\mu_i \equiv i \pmod{r}$, viz., $p\mu_i + i \equiv 0$, then

$$g_1 = \frac{\mu_1}{1} + \frac{\mu_2}{2} + \dots + \frac{\mu_{r-1}}{r-1} + \frac{\mu_1}{r+1} + \frac{\mu_2}{r+2} + \dots + \frac{\mu_{r-1}}{2r-1} + \frac{\mu_1}{2r+1} + \dots$$

Set $\mu_r = 0$, $\mu_{i+jr} = \mu_i$. Then

$$g_n = \sum_{i=1}^{p-1} \left(\frac{\mu_i}{i}\right)^n, \quad \sum_{i=1}^{p-1} \frac{\mu_i}{i^2} \equiv 0 \pmod{p}.$$

Sylvester's corrected results are proved. From $(1+1)^p$,

$$\frac{2^p - 2}{p} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{p-1} \equiv 2 \left(1 + \frac{1}{3} + \dots + \frac{1}{p-2}\right) \pmod{p}.$$

For $r' = r + kp$, let μ_i' be the positive root of $p\mu_i' + i \equiv 0 \pmod{r'}$. Then

$$r'^{p-1} = 1 + h_1 p + \frac{1}{2}(h_1^2 - h_2)p^2 + \dots, \quad h_n = \sum_{i=1}^{p-1} \left(\frac{\mu_i'}{i}\right)^n.$$

It is shown that, for some integer t ,

$$h_1 - g_1 + \frac{k}{r} = tp, \quad h_2 - g_2 \equiv -2\frac{k}{r} - \frac{k^2}{r^2} + 2t \equiv \frac{2k}{r}g_1 - \frac{k^2}{r^2} \pmod{p},$$

$$r'^{p(p-1)} \equiv 1 + g_1 p^{i+1} - \frac{1}{2}g_2 p^{i+2} \pmod{p^{i+3}}.$$

Glaisher,¹⁷ using the same notations, gave

$$r^{p-1} \equiv 1 + p \left(\frac{\mu_1}{1} + \frac{\mu_2}{2} + \dots + \frac{\mu_{p-1}}{p-1} \right) \pmod{p^2}.$$

¹⁵L'intermédiaire des math., 8, 1901, 122, 205-6 (7, 1900, 357).

^{15a}Ibid., 214-5.

¹⁶Quar. Jour. Math., 32, 1901, 1-27, 240-251.

¹⁷Messenger Math., 30, 1900-1, 78.

Glaisher¹⁸ considered q_u in connection with Bernoullian numbers and gave

$$\frac{3^{p-1}-1}{p} \equiv -\frac{2}{3} \left(1 + \frac{1}{2} + \dots + \frac{1}{k}\right) \pmod{p=3k+1}.$$

A. Pleskot¹⁹ duplicated the work of Plana.⁶

P. Bachmann²⁰ gave an exposition of the work by Sylvester,⁵ Stern,⁸ Mirimanoff.¹²

M. Lerch²¹ set, for any odd integer p and for u prime to p ,

$$q_u = \frac{1}{p}(u^{p(p)} - 1).$$

Then,* as a generalization of (2),

$$\begin{aligned} q_{uv} &\equiv q_u + q_v, & q_{u+pv} &\equiv q_u + \frac{v\phi(p)}{u} \pmod{p}, \\ q_u &\equiv \sum_{\nu} \frac{1}{u\nu} \left[\frac{u\nu}{p} \right], & 2q_2 &\equiv \sum_{\lambda} \frac{1}{\lambda} \equiv -\sum_{\mu} \frac{1}{\mu} \pmod{p}, \end{aligned}$$

where ν ranges over the positive integers $< p$ and prime to p ; λ over those $> p/2$; μ over those $< p/2$. Henceforth, let p be an odd prime and set $N = \{(p-1)! + 1\}/p$. Then $N \equiv q_1 + \dots + q_{p-1}$,

$$q_2 \equiv -\frac{1}{3} \sum_{\nu=1}^{[p/4]} \frac{1}{\nu}, \quad 3q_3 \equiv -2 \sum_{\nu=1}^{[p/3]} \frac{1}{\nu}, \quad 5q_5 \equiv -2 \sum_{a=1}^{[p/5]} \frac{1}{a} - 2 \sum_{b=1}^{[2p/5]} \frac{1}{b},$$

modulo p . If $\psi(n)$ is the number of sets of positive solutions $< p$ of $\mu\nu = n$ and hence the number of divisors between n/p and p of n ,

$$N \equiv \sum_{n=1}^{(p-1)^2} \frac{\psi(n)}{n} \left[\frac{n}{p} \right] \pmod{p}.$$

Employing Legendre's symbol and Bernoullian numbers, we have

$$A = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p} \right) q_{\nu} \equiv 0 \text{ or } (-1)^{n-1} 2B_n \pmod{p},$$

according as $p = 4n+3$ or $4n+1$. In the respective cases,

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p} \right) p q_{\nu} \equiv Cl(-p) \text{ or } 0 \pmod{p},$$

where $Cl(-\Delta)$ is the number of classes of positive primitive forms $ax^2 + bxy + cy^2$ of negative discriminant $b^2 - 4ac = -\Delta$. Also, modulo p ,

$$A - N \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu^2} \left[\frac{\nu^2}{p} \right], \quad q_a \equiv 2 \sum_{a} \frac{1}{aa} \left[\frac{aa}{p} \right],$$

$$q_a \equiv 2 \sum_b \frac{1}{ab} \left[\frac{ab}{p} \right], \quad q_b \equiv 2 \sum_a q_a - 2 \sum_{\beta} q_{\beta} + 2 \sum_a \frac{1}{ab} \left[\frac{ab}{p} \right],$$

where a, a are quadratic residues of p , and b, β non-residues.

¹⁸Proc. London Math. Soc., 33, 1900-1, 49-50.

¹⁹Zeitschrift für das Realschulwesen, Wien, 27, 1902, 471-2.

²⁰Niedere Zahlentheorie, I, 1902, 159-169.

*The greatest integer $\leq x$ is denoted by $[x]$.

²¹Math. Annalen, 60, 1905, 471-490.

H. F. Baker²² extended Sylvester's theorem to any modulus N :

$$\frac{r^{\varphi(N)} - 1}{N} \equiv \sum_{i=1}^{\varphi(N)} \frac{\{N'm_i\}}{N - m_i} \pmod{N},$$

where the m_i denote the integers $< N$ and prime to N , $N'N \equiv 1 \pmod{r}$, and $\{k\}$ is the least positive residue modulo r of k .

Lerch²³ extended Mirimanoff's¹² formula to the case of a composite modulus m . Set

$$q(a, m) = \frac{1}{m}(a^{\varphi(m)} - 1).$$

Let a belong to the exponent $\phi(m)/e$. Then $q(a, m) \equiv e \sum \alpha/\beta \pmod{m}$, where β ranges over the residues of the incongruent powers of a , and $m\alpha + \beta \equiv 0 \pmod{a}$, $0 \leq \alpha < a$. As an extension of Sylvester's theorem,

$$q(a, m) \equiv \sum_{\nu} \frac{r_{\nu}}{\nu} \equiv -\sum_{\nu} \frac{r'_{\nu}}{\nu} \pmod{m},$$

where ν ranges over the integers $< m$ and prime to m , while

$$mr_{\nu} + \nu \equiv 0, \quad mr'_{\nu} - \nu \equiv 0 \pmod{a}, \quad 0 \leq r_{\nu} < a, \quad 0 \leq r'_{\nu} < a.$$

For $m = m_1 \dots m_k$, where the m_j are relatively prime,

$$q(a, m) \equiv \sum_{j=1}^k n_j n'_j \phi(n_j) q(a, m_j) \pmod{m},$$

where $m = m_j n_j$, $n_j^2 n'_j \equiv 1 \pmod{m_j}$.

H. Hertz²⁴ verified that, for $a < p < 307$, $a^{p-1} - 1$ is divisible by p^3 only for $a = 68$, $p = 113$; $a = 3, 9$, $p = 11$. He examined all the primes between 307 and 751, but only for a and $p - a$ when $a < \sqrt{p}$, finding only $p = 113$, $a = 68$. Removing the restriction $a < \sqrt{p}$, he found only the solutions

$$\begin{aligned} p = 11, a = 3; \quad p = 331, a = 18, 71; \quad p = 353, a = 14; \\ p = 487, a = 10, 175; \quad p = 673, a = 22, \end{aligned}$$

together with the square of each a .

A. Friedmann and J. Tamarkine²⁵ gave formulas connecting q_u with Bernoullian numbers and $[u/p]$.

A. Wieferich²⁶ proved that if $x^p + y^p + z^p = 0$ is satisfied by integers x, y, z prime to p , where p is an odd prime, then $2^{p-1} \equiv 1 \pmod{p^2}$. Shorter proofs were given by D. Mirimanoff²⁷ and G. Frobenius.²⁸

D. A. Grave²⁹ gave the residue of q_2 for each prime $p < 1000$ and thought he could prove that $2^p - 2$ is never divisible by p^2 (error, Meissner³³).

A. Cunningham³⁰ verified that $2^p - 2$ is not divisible by p^2 for any prime $p < 1000$, and³¹ that $3^p - 3$ is not divisible by p^2 for a prime $p = 2^a 3^b + 1 < 100$.

W. H. L. Janssen van Raay³² noted that $2^p - 2$ is not divisible by p^2 in general.

²²Proc. London Math. Soc., (2), 4, 1906, 131-5.

²³Comptes Rendus Paris, 142, 1906, 35-38.

²⁴Archiv Math. Phys., (3), 13, 1908, 107.

²⁵Jour. für Math., 135, 1909, 146-156.

²⁶Jour. für Math., 136, 1909, 293-302.

²⁷L'enseignement math., 11, 1909, 455-9.

²⁸Sitzungsber. Ak. Wiss. Berlin, 1909, 1222-4; reprinted in Jour. für Math., 137, 1910, 314.

²⁹An elementary text on the theory of numbers (in Russian), Kiev, 1909, p. 315; Kiev Izv. Univ., 1909, Nos. 2-10.

³⁰Report British Assoc. for 1910, 530. L'intermédiaire des math., 18, 1911, 47; 19, 1912, 159. Proc. London Math. Soc., (2), 8, 1910, xiii.

³¹L'intermédiaire des math., 18, 1911, 47. Cf., 20, 1913, 206.

³²Nieuw Archief voor Wiskunde, (2), 10, 1912, 172-7.

L. Bastien^{32a} verified that (1) holds for $p < 50$ only for $p = 43$, $a = 19$, and for Jacobi's² cases. He stated that, if $p = 4p \pm 1$ is a prime,

$$-\frac{1}{2}q_2 \equiv 1 + 1/3 + 1/5 + \dots + 1/(2h-1) \pmod{p}.$$

W. Meissner³³ gave a table showing the least positive residue of $(2^t-1)/p$ modulo p for each prime $p < 2000$, where t is the exponent to which 2 belongs modulo p . In particular, 2^p-2 is divisible by the square of the prime $p = 1093$, contrary to Proth⁷ and Grave,²⁹ but for no other $p < 2000$.

In the chapter on Fermat's last theorem will be given not only the condition $q_2 \equiv 0 \pmod{p}$ of Wieferich²⁶ but also $q_3 \equiv 0 \pmod{p}$, etc., with citations to D. Mirimanoff, *Comptes Rendus Paris*, 150, 1910, 204-6, and *Jour. für Math.*, 139, 1911, 309-324; H. S. Vandiver, *ibid.*, 144, 1914, 314-8; G. Frobenius, *Sitzungsber. Ak. Wiss. Berlin*, 1910, 200-8; 1914, 653-81. These papers give further properties of q_u .

P. Bachmann³⁴ employed the identity

$$\begin{aligned} & (a+b+c)^p - (a+b-c)^p + (a-b-c)^p - (a-b+c)^p \\ &= 2 \binom{p}{1} c \{ (a+b)^{p-1} - (a-b)^{p-1} \} + 2 \binom{p}{3} c^3 \{ (a+b)^{p-3} - (a-b)^{p-3} \} + \dots \end{aligned}$$

for $a=b=1$, $c=2$ or 1 to get expressions for q_2 or q_3 , whence

$$\frac{3^p-3}{p} \equiv 2 \left\{ \frac{2^{p-1}}{1} + \frac{2^{p-3}}{3} + \frac{2^{p-5}}{5} + \dots + \frac{2^2}{p-2} \right\} \pmod{p},$$

for an odd prime p . Comparing this with the value of $(3^p-3)/p$ obtained by expanding $(2+1)^p$, we see that

$$\frac{2^p-2}{p} \equiv 2^{p-1} + \frac{1}{2} \cdot 2^{p-2} + \frac{1}{3} \cdot 2^{p-3} + \dots + \frac{1}{p-1} \cdot 2 \pmod{p}.$$

Again,

$$q_2 \equiv 2 - \left(\frac{p-1}{2} \right)^2 + \sum \text{sgn.}(s-t) (-1)^{s+t+1} s \pmod{p},$$

summed for all sets of solutions of $s^2 \equiv t^2 + 1 \pmod{p}$. Finally,

$$q_2 \equiv \sum_{h=1}^{p-1} \left\{ (r^h - r^{-h}) \sum_{\theta} (r^{2\theta h} - 1)^{-1} \right\},$$

where r is a primitive p th root of unity.

*H. Brocard³⁵ commented on $a^{p-1} \equiv 1 \pmod{p^n}$. *H. G. A. Verkaart³⁶ treated the divisibility of $a^p - a$ by p . E. Fauquembergue³⁷ checked that $2^p \equiv 2 \pmod{p^2}$ for $p = 1093$.

N. G. W. H. Beeger³⁸ tabulated all roots of $x^{p-1} \equiv 1 \pmod{p^2}$ for each prime $p < 200$. If ω is a primitive root of p^2 , the absolutely least residue

^{32a}Sphinx-Oedipe, 7, 1912, 4-6. It is stated that G. Tarry had verified in 1911 that 2^p-2 is not divisible by a prime $p < 1013$.

³³Sitzungsber. Ak. Wiss. Berlin, 1913, 663-7.

³⁴Jour. für Math., 142, 1913, 41-50.

³⁵Revista de la Sociedad Mat. Española, 3, 1913-4, 113-4.

³⁶Wiskundig Tijdschrift, vol. 2, 1906, 238-240.

³⁷L'intermédiaire des math., 1914, 33.

³⁸Messenger Math., 43, 1913-4, 72-84.

$\pm x_1$ modulo p^2 of ω^p is a root, that $(\pm x_2)$ of x_1^2 is a second root, that $(\pm x_3)$ of $x_1 x_2$ is a third root, etc., until the root $\pm x_s$ is reached, where $s = (p-1)/2$. The remaining roots are $p^2 - x_i (i=1, \dots, s)$. He proved that

$$(x_1 \dots x_s)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p^2}.$$

Hence $x_1 \dots x_s \equiv \pm 1$ if $p = 4n+1$.

W. Meissner³⁹ wrote h_m for the residue $< p^m$ of h^{p^m-1} modulo p^m . When h varies from 1 to $p-1$, we get $p-1$ roots h_m of $x^{p^m-1} \equiv 1 \pmod{p^m}$. The product of the roots given by $h=1, \dots, (p-1)/2$, is $\equiv (-1)^z$ or $(-1)^z \sigma \pmod{p^m}$, according as $p=4n-1$ or $4n+1$, where z is the number of pairs of integers $< p/2$ whose product is $\equiv -1 \pmod{p}$, and σ is the smaller of the two roots of $x^2 \equiv -1 \pmod{p}$. No number $< p$ which belongs to one of the exponents 2, 3, 4, 6, modulo p , can be a root of $x^{p-1} \equiv 1 \pmod{p^2}$. A root of the latter is given for each prime $p < 300$, and a root modulo p^3 for each $p < 200$; also the exponent to which each root belongs.

N. Nielsen⁴⁰ noted that, if we select $2r$ distinct integers $a_s, b_s (s=1, \dots, r)$ from $1, \dots, p-1$, such that $a_s + b_s = p$, then

$$\frac{a_1 \dots a_r}{b_1 \dots b_r} = (-1)^r (1 - pA), \quad A \equiv \sum_{s=1}^r \frac{1}{b_s} \equiv \sum_{s=1}^r (q_{a_s} - q_{b_s}) \pmod{p}.$$

Proof is given of various results by Lerch,²¹ also of simple relations between q_a and Bernoullian numbers, and of the final formula by Plana,⁶ here attributed to Euler.⁴¹

H. S. Vandiver⁴² proved that there are not fewer than $[\sqrt{p}]$ and not more than $p - (1 + \sqrt{2p-5})/2$ incongruent least positive residues of $1, 2^{p-1}, \dots, (p-1)^{p-1}$, modulo p^2 .

N. Nielsen⁴³ noted that, if a is not divisible by the odd prime p ,

$$q_a \equiv \frac{a-1}{2a} + \sum_{s=1}^{(p-3)/2} \frac{1}{2s} (-1)^{s-1} B_s (a^{p-2s-1} - 1) \pmod{p},$$

$$q_1 + q_2 + \dots + q_{p-1} \equiv (-1)^{n-1} B_n + \frac{1}{p} - 1 \pmod{p^2}, \quad n = (p-1)/2.$$

W. Meissner⁴⁴ gave various expressions for q_2 and q_3 .

A. Gérardin⁴⁵ found all primes $p < 2000$, including those of the form $2^n - 1$, for which q_2 is symmetrical when written to the base 2.

H. S. Vandiver⁴⁶ proved that $q_2 \equiv 0 \pmod{p^2}$ if and only if

$$1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \equiv 0 \pmod{p^2}.$$

He gave various expressions for $(n^k - 1)/m$.

³⁹Sitzungsber. Berlin Math. Gesell., 13, 1914, 96-107.

⁴⁰Ann. sc. l'école norm. sup., (3), 31, 1914, 171-9.

⁴¹Euler, Institutiones Calculi Diff., 1755, 406. Proof, Math. Quest. Educ. Times, 48, 1888, 48.

⁴²Bull. Amer. Math. Soc., 22, 1915, 61-7.

⁴³Oversigt Danske Vidensk. Selsk. Forhandling, 1915, 518-9, 177-180; cf. Lerch's²¹ N.

⁴⁴Mitt. Math. Gesell. Hamburg, 5, 1915, 172-6, 180.

⁴⁵Nouv. Ann. Math., (4), 17, 1917, 102-8.

⁴⁶Annals of Math., 18, 1917, 112.

CHAPTER V.

EULER'S ϕ -FUNCTION, GENERALIZATIONS, FAREY SERIES.

NUMBER $\phi(n)$ OF INTEGERS $< n$ AND PRIME TO n .

L. Euler,¹ in connection with his generalization of Fermat's theorem, investigated the number $\phi(n)$ of positive integers not exceeding n which are relatively prime to n , without then using a functional notation for $\phi(n)$. He began with the theorem that, if the n terms $a, a+d, \dots, a+(n-1)d$ in arithmetical progression are divided by n , the remainders are $0, 1, \dots, n-1$ in some order, provided d is prime to n ; in fact, no two of the terms have the same remainder.

If p is a prime, $\phi(p^m) = p^{m-1}(p-1)$, since $p, 2p, \dots, p^{m-1} \cdot p$ are the only ones of the p^m positive integers $\leq p^m$ not prime to p^m . To prove that

$$(1) \quad \phi(AB) = \phi(A)\phi(B) \quad (A, B \text{ relatively prime}),$$

let $1, a, \dots, \omega$ be the integers $< A$ and prime to A . Then the integers $< AB$ and prime to A are

1	a	\dots	ω
$A+1$	$A+a$	\dots	$A+\omega$
$2A+1$	$2A+a$	\dots	$2A+\omega$
$\dots\dots\dots$	$\dots\dots\dots$	\dots	$\dots\dots\dots$
$(B-1)A+1$	$(B-1)A+a$	\dots	$(B-1)A+\omega$

The terms in any column form an arithmetical progression whose difference A is prime to B , and hence include $\phi(B)$ integers prime to B . The number of columns is $\phi(A)$. Hence there are $\phi(A)\phi(B)$ positive integers $< AB$, prime to both A and B , and hence prime to AB . If p, \dots, s are distinct primes, the two theorems give

$$(2) \quad \phi(p^\lambda \dots s^\epsilon) = p^{\lambda-1}(p-1) \dots s^{\epsilon-1}(s-1).$$

Euler² later used πN to denote $\phi(N)$ and gave a different proof of (2). First, let $N = p^n q$, where p, q are distinct primes. Among the $N-1$ integers $< N$ there are p^n-1 multiples of q , and $p^{n-1}q-1$ multiples of p , these sets having in common the $p^{n-1}-1$ multiples of pq . Hence

$$\phi(N) = N-1 - (p^n-1) - (p^{n-1}q-1) + p^{n-1}-1 = p^{n-1}(p-1)(q-1).$$

A simpler proof is then given for the modified form of (2):

$$(3) \quad \phi(N) = \frac{N(p-1)(q-1) \dots (s-1)}{pq \dots s},$$

where p, q, r, \dots, s are the distinct primes dividing N . There are N/p multiples $< N$ of p and hence $N' = N(p-1)/p$ integers $< N$ and prime to p . Of these, N'/q are divisible by q ; excluding them, we have $N'' = N'(q-1)/q$ numbers $< N$ and prime to both p and q . The r th part of these are said

¹Novi Comm. Ac. Petrop., 8, 1760-1, 74; Comm. Arith., 1, 274. Opera postuma, I, 492-3.

²Acta Ac. Petrop., 4 II (or 8), 1780 (1755), 18; Comm. Arith., 2, 127-133. He took $\phi(1)=0$.

[cf. Poinso¹⁶] to be divisible by r ; after excluding them we get $N''(r-1)/r$ numbers; etc.

Euler³ noted in a posthumous paper that, if p, q, r are distinct primes, there are r multiples $\leq pqr$ of pq , and qr multiples of p , and a single multiple of pqr , whence

$$\phi(pqr) = pqr - qr - pr - pq + r + p + q - 1 = (p-1)(q-1)(r-1).$$

In general, if M is any number not divisible by the prime p , and if μ denotes the number of integers $\leq M$ and prime to M , there are $M-\mu$ integers $\leq M$ and not prime to M and hence $p^n(M-\mu)$ integers $\leq Mp^n$ and not prime to M and therefore not prime to Mp^n . Of the Mp^{n-1} multiples $\leq Mp^n$ of p , exclude the $p^{n-1}(M-\mu)$ which are not prime to M ; we obtain $p^{n-1}\mu$ multiples of p which are prime to M . Hence

$$\phi(p^n M) = p^n M - p^n(M-\mu) - p^{n-1}\mu = p^{n-1}(p-1)\mu.$$

A. M. Legendre⁴ noted that, if θ, \dots, ω are any odd primes not dividing A , the number of terms of the progression $A+B, 2A+B, \dots, nA+B$ which are divisible by no one of the primes θ, \dots, ω is approximately $n(1-1/\theta) \dots (1-1/\omega)$, and exactly that number if n is divisible by θ, \dots, ω .

C. F. Gauss⁵ introduced the symbol $\phi(N)$. He expressed Euler's¹ proof of (1) in a different form. Let α be any one of the $\phi(A)$ integers $< A$ and prime to A , while β is any one of the $\phi(B)$ integers $< B$ and prime to B . There is one and but one positive integer $x < AB$ such that $x \equiv \alpha \pmod{A}$, $x \equiv \beta \pmod{B}$. Since this x is prime to A and to B , it is prime to AB .

Making the agreement that $\phi(1) = 1$, Gauss proved

$$(4) \quad \Sigma \phi(d) = N \quad (d \text{ ranging over the divisors of } N).$$

For each d , multiply the integers $\leq d$ and prime to d by N/d ; we obtain $\Sigma \phi(d)$ integers $\leq N$, proved to be distinct and to include $1, 2, \dots, N$.

A. M. Legendre⁶ proved (3) as follows: First, let $N = pM$, where p is a prime which may or may not divide M ; then $Mp-M$ of the numbers $1, \dots, N$ are not divisible by p . Second, let $N = pqM$, where p and q are distinct primes. Then $1, \dots, N$ include M numbers divisible by both p and q ; $Mp-M$ numbers divisible by q and not by p ; $Mq-M$ numbers divisible by p and not by q . Hence there remain $N(1-1/p)(1-1/q)$ numbers divisible by neither p nor q . Third, a like argument is said to apply to $N = pqrM$, etc.

Legendre (p. 412) proved that if A, C are relatively prime and if $\theta, \lambda, \mu, \dots, \omega$ are odd primes not dividing A , the number of terms $kA - C$ ($k = 1, \dots, n$), which are divisible by no one of θ, \dots, ω , is

$$n - \Sigma \left[\frac{n + \theta_0}{\theta} \right] + \Sigma \left[\frac{n + (\theta\lambda)_0}{\theta\lambda} \right] - \Sigma \left[\frac{n + (\theta\lambda\mu)_0}{\theta\lambda\mu} \right] + \dots,$$

¹⁶Tractatus de numerorum, Comm. Arith., 2, 515-8. Opera postuma, I, 1862, 16-17.

³Essai sur la théorie des nombres, 1798, p. 14.

⁴Disquisitiones Arithmeticae, 1801, Arts. 38, 39.

⁵Théorie des nombres, ed. 2, 1808, 7-8; German trans. of ed. 3 by Maser, 8-10.

where the summations extend over the combinations of θ, \dots, ω taken $1, 2, \dots$, at a time, while Δ_0 is a positive integer $< \Delta$ for which $A\Delta_0 + C$ is divisible by Δ , and $[x]$ is the greatest integer $\leq x$. We thus derive the approximation stated by Legendre.⁴ Taking $A=1$, $C=0$ (p. 420), we see that the number of integers $\leq n$, which are divisible by no one of the distinct primes $\theta, \lambda, \dots, \omega$ is

$$(5) \quad n - \Sigma \left[\frac{n}{\theta} \right] + \Sigma \left[\frac{n}{\theta\lambda} \right] - \Sigma \left[\frac{n}{\theta\lambda\mu} \right] + \dots$$

A. von Ettingshausen⁷ reproduced without reference Euler's² proof of (3) and gave an obscurely expressed proof of (4). Let $N = p^a q^b \dots$, where p, q, \dots are distinct primes. Consider first only the divisors $d = p^\mu q^\nu$, where $\mu > 0, \nu > 0$, so that d involves the primes p and q , but no others. By (3),

$$\phi(d) = d \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{q} \right), \quad \sum_{\mu=1}^a \sum_{\nu=1}^b p^\mu q^\nu = (p + p^2 + \dots + p^a)(q + \dots + q^b),$$

$$\Sigma \phi(p^\mu q^\nu) = (p^a - 1)(q^b - 1).$$

Similarly, $\Sigma \phi(p^\mu) = p^a - 1$. In this way we treat together the divisors of N which involve the same prime factors. Hence when d ranges over all the divisors of N ,

$$\Sigma \phi(d) = 1 + \sum_p (p^a - 1) + \sum_{p, q} (p^a - 1)(q^b - 1) + \sum_{p, q, r} (p^a - 1)(q^b - 1)(r^c - 1) + \dots$$

$$= \prod_p \{ 1 + (p^a - 1) \} = \prod p^a = N,$$

where the summation indices range over the combinations of all the prime factors of N taken $1, 2, \dots$ at a time. [Cf. Sylvester.³²]

A. L. Crelle⁸ considered the number z_j of integers, chosen from n_1, \dots, n_a , which are divisible by exactly j of the distinct primes p_1, \dots, p_m ; and the number s_j of the integers, chosen from n_1, \dots, n_a , which are divisible by at least j of the primes p_i . Then

$$z_1 + z_2 + \dots + z_m = s_1 - s_2 + s_3 - \dots \pm s_m.$$

Let ν be the number of the integers n_1, \dots, n_a which are divisible by no one of the primes p_i . Then

$$a = \Sigma z_i + \nu, \quad \nu = a - s_1 + s_2 - \dots \mp s_m.$$

In particular, take n_1, \dots, n_a to be $1, 2, \dots, N$, where $N = p^a q^b r^c \dots$, and take p_1, \dots, p_m to be p, q, r, \dots . Then

$$s_1 = \frac{N}{p} + \frac{N}{q} + \dots, \quad s_2 = \frac{N}{pq} + \frac{N}{pr} + \dots, \quad s_3 = \frac{N}{pqr} + \dots,$$

$$\phi(N) = N - s_1 + s_2 - \dots = N \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{q} \right) \dots$$

He proved (1) for $B = a^a$, where a is a prime not dividing A (p. 40). By Euler's¹ table there are $B\phi(A)$ integers $< AB$ and prime to A . In Euler's

⁷Zeitschrift für Physik u. Math. (eds., Baumgartner and Ettingshausen), Wien, 5, 1829, 287-292.

⁸Abh. Akad. Wiss. Berlin (Math.), 1832, 37-50.

notation, $a(kA+1)$, $a(kA+a)$, \dots , $a(kA+\omega)$ give all the numbers between kaA and $(k+1)aA$ which are divisible by a and are prime to A . Taking $k=0, 1, \dots, a^{a-1}-1$, we see that there are exactly $a^{a-1}\phi(A)$ multiples of a which are $<AB$ and prime to A . Hence

$$\phi(a^a A) = a^a \phi(A) - a^{a-1} \phi(A) = \phi(a^a) \phi(A).$$

F. Minding⁹ proved Legendre's formula (5). The number of integers $\leq n$, not divisible by the prime θ , is $n - [n/\theta]$. To make the general step by induction, let p_1, \dots, p_k be distinct primes, and denote by $(B; p_1, \dots, p_k)$ the number of integers $\leq B$ which are divisible by no one of the primes p_1, \dots, p_k . Then, if p is a new prime,

$$(B; p_1, \dots, p_k, p) = (B; p_1, \dots, p_k) - ([B/p]; p_1, \dots, p_k).$$

The truth of (4) for the special case $N=p-1$, where p is a prime, follows (p. 41) from the fact that $\phi(d)$ numbers belong to the exponent d modulo p if d is any divisor of $p-1$.

N. Druckenmüller¹⁰ evaluated $\phi(b)$, first for the case in which b is a product $cd \dots kl$ of distinct primes. Set $b = \beta l$ and denote by $\psi(b)$ the number of integers $< b$ having a factor in common with b . There are $l\psi(\beta)$ numbers $< b$ which are divisible by one of the primes c, \dots, k , since there are $\psi(\beta)$ in each of the sets

$$1, 2, \dots, \beta; \beta+1, \dots, 2\beta; \dots; (l-1)\beta+1, \dots, l\beta.$$

Again, $l, 2l, \dots, \beta l$ are the integers $< b$ with the factor l . Of these, $\phi(\beta)$ are prime to β , while the others have one of the factors c, \dots, k and occur among the above $l\psi(\beta)$. Hence $\psi(b) = l\psi(\beta) + \phi(\beta)$. But $\psi(\beta) + \phi(\beta) = \beta$. Hence

$$\phi(b) = (l-1)\phi(\beta) = (c-1) \dots (l-1).$$

Next, let b be a product of powers of c, d, \dots, l , and set $b = L\beta$, $\beta = cd \dots l$. By considering L sets as before, we get

$$\psi(b) = L\psi(\beta), \quad \phi(b) = L\phi(\beta).$$

E. Catalan¹¹ proved (4) by noting that

$$\Sigma \phi(p^\alpha q^\beta \dots) = \Pi \{1 + \phi(p) + \dots + \phi(p^\alpha)\} = \Pi p^\alpha = N,$$

where there are as many factors in each product as there are distinct prime factors of N .

A. Cauchy¹² gave without reference Gauss's⁵ proof of (1).

E. Catalan¹³ evaluated $\phi(N)$ by Euler's² second method.

C. F. Arndt¹⁴ gave an obscure proof of (4), apparently intended for Catalan's.¹¹ It was reproduced by Desmarest, *Théorie des nombres*, 1852, p. 230.

⁹Anfangsgründe der Höheren Arith., 1832, 13-15.

¹⁰Theorie der Kettenreihen... Trier, 1837, 21.

¹¹Jour. de Mathématiques, 4, 1839, 7-8.

¹²Comptes Rendus Paris, 12, 1841, 819-821; Exercices d'analyse et de phys. math., Paris, 2, 1841, 9; Oeuvres, (2), 12.

¹³Nouv. Ann. Math., 1, 1842, 466-7.

¹⁴Archiv Math. Phys., 2, 1842, 6-7.

J. A. Grunert¹⁵ examined in a very elementary way the sets

$$jk+1, \quad jk+2, \dots, \quad jk+k-1, \quad (j+1)k \quad (j=0, 1, \dots, p-1)$$

and proved that $\phi(pk) = p\phi(k)$ if the prime p divides k , while $\phi(pk) = (p-1)\phi(k)$ if the prime p does not divide k . From these results, (2) is easily deduced [cf. Crelle¹⁷ on $\phi(Z)$].

L. Poinso¹⁶ gave Catalan's¹¹ proof of (4) and proved the statements made by Euler² in his proof of (3). Thus to show that, of the $N' = N(1-1/p)$ integers $< N$ and prime to p , exactly N'/q are divisible by q , note that the set $1, \dots, N$ contains N/q multiples of q and the set $p, 2p, \dots$ contains $(N/p)/q$ multiples of q , while the difference is N'/q .

If P, Q, R, \dots are relatively prime in pairs, any number prime to $N = PQR \dots$ can be expressed in the form

$$pQR \dots + qPR \dots + rPQ \dots + \dots,$$

where p is prime to P , q to Q , etc. If also $p < P$, $q < Q$, etc., no two of these sums are equal. Thus there are $\phi(P)\phi(Q) \dots$ such sums [certain of which may exceed N].

To prove (4), take (pp. 70-71) a prime p of the form $kN+1$ and any one of the N roots ρ of $x^N \equiv 1 \pmod{p}$. Then there is a least integer d , a divisor of N , such that $\rho^d \equiv 1 \pmod{p}$. The latter has $\phi(d)$ such roots. Also ρ is a primitive root of the last congruence and of no other such congruence whose degree is a divisor of N .

A. L. Crelle¹⁷ considered the product $E = e_1 e_2 \dots e_n$ of integers relatively prime in pairs, and set $E_i = E/e_i$. When x ranges over the values $1, \dots, e_i$, the least positive residue modulo E of $E_1 x_1 + \dots + E_n x_n$ takes each of the values $1, \dots, E$ once and but once. In case x_i is prime to e_i for $i=1, \dots, n$, the residue of $\Sigma E_i x_i$ is prime to E and conversely. Let d_{i1}, d_{i2}, \dots be any chosen divisors > 1 of e_i which are relatively prime in pairs. Let $\psi(e_i)$ denote the number of integers $\leq e_i$ which are divisible by no one of the d_{i1}, d_{i2}, \dots . Let $\psi(E)$ be the number of integers $\leq E$ which are divisible by no one of the $d_{11}, d_{12}, d_{21}, \dots$, including now all the d 's. Then $\psi(E) = \psi(e_1) \dots \psi(e_n)$. In case d_{i1}, d_{i2}, \dots include all the prime divisors > 1 of e_i , $\psi(e_i)$ becomes $\phi(e_i)$. Of the two proofs (pp. 69-73), one is based on the first result quoted, while the other is like that by Gauss.⁵

As before, let $\psi(y)$ be the number of integers $\leq y$ which are divisible by no one of certain chosen relatively prime divisors d_1, \dots, d_m of y . By considering the xy numbers $ny+r$ ($0 \leq n < x$, $1 \leq r \leq y$), it is proved (p. 74) that, when x and y are relatively prime,

$$\psi(xy) = x\psi(y), \quad \psi_2(xy) = (x-1)\psi(y),$$

where $\psi_2(xy)$ is the number of integers $\leq xy$ which are divisible neither by x nor by any one of the d 's. These formulas lead (pp. 79-83) to the value of $\phi(Z)$. Set

$$Z = p_1^{e_1} \dots p_\mu^{e_\mu}, \quad z = p_1 \dots p_\mu, \quad n = Z/z,$$

¹⁵Archiv. Math. Phys., 3, 1843, 196-203.

¹⁶Jour. de Mathématiques, 10, 1845, 37-43.

¹⁷Encyklopädie der Zahlentheorie, Jour. für Math., 29, 1845, 58-95.

where p_1, \dots, p_μ are distinct primes. For a prime p , not dividing y , we have $\phi(py) = (p-1)\phi(y)$. Take $y = p_1$, $p = p_2$; then

$$\phi(p_1 p_2) = (p_1 - 1)(p_2 - 1).$$

Next, take $y = p_1 p_2$, $p = p_3$, and use also the last result; thus

$$\phi(p_1 p_2 p_3) = (p_1 - 1)(p_2 - 1)(p_3 - 1),$$

and similarly for $\phi(z)$. When ζ ranges over the integers $< z$ and prime to z , the numbers $\nu z + \zeta$ ($\nu = 0, 1, \dots, n-1$) give without repetition all the integers $< Z$ and prime to Z . Hence $\phi(Z) = n\phi(z)$, which leads to (2). [Cf. Guilmin,²³ Steggall.⁷⁸]

The proofs of (4) by Gauss⁵ and Catalan¹¹ are reproduced without references (pp. 87-90). A third proof is given. Set $N = a^\alpha b^\beta c^\gamma \dots$, where a, b, c, \dots are distinct primes. Consider any divisor $\epsilon = b^{\beta_1} c^{\gamma_1} \dots$ of N such that ϵ is not divisible by a . Then

$$\phi(\epsilon a^k) = a^{k-1}(a-1)\phi(\epsilon).$$

Sum for $k = 0, 1, \dots, a$; we get $a^\alpha \phi(\epsilon)$. When k ranges over its values and β_1 over the values $0, 1, \dots, \beta$, and γ_1 over the values $0, 1, \dots, \gamma$, etc., ϵa^k ranges over all the divisors d of N . Hence $\Sigma \phi(d) = a^\alpha \Sigma \phi(\epsilon)$. Similarly, if ϵ_1 range over the divisors not divisible by a or b ,

$$\Sigma \phi(\epsilon) = b^\beta \Sigma \phi(\epsilon_1), \dots, \quad \Sigma \phi(d) = a^\alpha b^\beta \dots = N.$$

E. Prouhet¹⁸ proposed the name indicator and symbol $i(N)$ for $\phi(N)$. He gave Gauss' proof of (1) and Catalan's proof of (4). If δ is the product of the distinct prime factors common to a and b ,

$$\phi(ab) = \phi(a)\phi(b)\delta/\phi(\delta).$$

As a generalization, let δ_i be the product of the distinct primes common to i of the numbers a_1, \dots, a_n ; then

$$\phi(a_1 \dots a_n) = \phi(a_1) \dots \phi(a_n) \frac{\delta_2}{\phi(\delta_2)} \frac{\delta_3^2}{\phi^2(\delta_3)} \dots \frac{\delta_n^{n-1}}{\phi^{n-1}(\delta_n)}.$$

Friderico Arndt¹⁹ proved (1) by showing that, if x ranges over the integers $< A$ and prime to A , while y ranges over the integers $< B$ and prime to B , then $Ay + Bx$ gives only incongruent residues modulo AB , each prime to AB , and they include every integer $< AB$ and prime to AB . [Crelle's¹⁷ first theorem for $n=2$.]

V. A. Lebesgue²⁰ used Euler's² argument to show that there are

$$\frac{N(p-1)(q-1) \dots (k-1)}{p \cdot q \dots k}$$

integers $< N$ and prime to p, q, \dots, k , the latter being certain prime divisors of N [Legendre,⁴ Minding⁹].

¹⁸Nouv. Ann. Math., 4, 1845, 75-80.

¹⁹Jour. für Math., 31, 1846, 246-8.

²⁰Nouv. Ann. Math., 8, 1849, 347.

G. L. Dirichlet²¹ added equations (4) for $N=n, \dots, 2, 1$, noting that, if $s \leq n$, $\phi(s)$ occurs in the new left member as often as there are multiples $\leq n$ of s . Hence

$$\sum_{s=1}^n \left[\frac{n}{s} \right] \phi(s) = \frac{1}{2}(n^2 + n).$$

The left member is proved equal to $\sum \psi[n/s]$, where

$$\psi(x) = \phi(1) + \dots + \phi(x).$$

It is then shown that $\psi(n) - 3n^2/\pi^2$ is of an order of magnitude not exceeding that of n^δ , where $2 > \delta > \gamma > 1$, γ being such that

$$\sum_{s=2}^{\infty} \frac{1}{s^\gamma} = 1.$$

P. L. Tchebychef²² evaluated $\phi(n)$ by showing that, if p is a prime not dividing A , the ratio of the number of integers $\leq pAN$ which are prime to A to the number which are prime to both A and p is $p:p-1$.

A. Guilmin²³ gave Crelle's¹⁷ argument leading to $\phi(Z)$.

F. Landry²⁴ proved (3). First, reject from $1, \dots, N$ the N/p multiples of p ; there remain $N(1-1/p)$ numbers prime to p . Next, to find how many of the multiples $q, 2q, \dots, N$ of q are prime to p , note that the coefficients $1, 2, \dots, N/q$ contain $N/q \cdot (1-1/p)$ integers prime to p by the first result, applied to the multiple N/q of p in place of N .

Daniel Augusto da Silva²⁵ considered any set S of numbers and denoted by $S(a)$ the subset possessing the property a , by $S(ab)$ the subset with the properties a and b simultaneously, by $(a)S$ the subset of numbers in S not having property a ; etc. Then

$$(a)S = S - S(a) = S\{1 - (a)\},$$

symbolically. Hence

$$(ba)S = (b)\{(a)S\} = S\{1 - (a)\}\{1 - (b)\},$$

$$(\dots cba)S = S\{1 - (a)\}\{1 - (b)\}\{1 - (c)\} \dots$$

A proof of the latter symbolic formula was given by F. Horta.^{25a}

With Silva, let S be the set $1, 2, \dots, n$, and let A, B, \dots be the distinct prime factors of n . Let properties a, b, \dots be divisibility by A, B, \dots . Then there are n/A terms in $S(a)$, $n/(AB)$ terms in $S(ab), \dots$, and $\phi(n)$ terms in $(\dots cba)S$. Hence our symbolic formula gives

$$\phi(n) = n \left(1 - \frac{1}{A}\right) \left(1 - \frac{1}{B}\right) \dots$$

²¹Abhand. Ak. Wiss. Berlin (Math.), 1849, 78-81; Werke, 2, 60-64.

²²Theorie der Congruenzen, 1889, §7; in Russian, 1849.

²³Nouv. Ann. Math., 10, 1851, 23.

²⁴Troisième mémoire sur la théorie des nombres, 1854, 23-24.

²⁵Propriedades geraes et resolucao directa das Congruencias binomias, Lisbon, 1854. Report on same by C. Alasia, Rivista di Fisica, Mat. e Sc. Nat., Pavia, 4, 1903, 13-17; reprinted in Annaes Scientificos Acad. Polyt. do Porto, Coimbra, 4, 1909, 166-192.

^{25a}Annaes de Sciencias e Lettras, Lisbon, 1, 1857, 705.

E. Betti²⁶ evaluated $\phi(m)$, where m is a product of powers of the distinct primes a_1, a_2, \dots . Consider the set C_i of the products of the a 's taken i at a time and their multiples $\leq m$. Thus C_0 is $1, \dots, m$, while C_2 is

$$a_1 a_2, 2a_1 a_2, \dots, \frac{m}{a_1 a_2} a_1 a_2; \quad a_1 a_3, 2a_1 a_3, \dots, \frac{m}{a_1 a_3} a_1 a_3; \dots$$

Let x be an integer $< m$ divisible by a_1, \dots, a_a . Then x occurs

$$1 + \binom{a}{2} + \binom{a}{4} + \dots = 2^{a-1}$$

times in the sets C_0, C_2, C_4, \dots ; and 2^{a-1} times in C_1, C_3, \dots . Summing

$$1 - \binom{a}{1} + \binom{a}{2} - \binom{a}{3} + \dots = 0$$

for each of the $m - \phi(m)$ integers $\leq m$ having factors in common with m , we get

$$m - \phi(m) - \Sigma \binom{a}{1} + \Sigma \binom{a}{2} - \dots = 0.$$

But $\Sigma \binom{a}{1}$ is the number of integers having in common with m one of the factors a_1, a_2, \dots , and hence equals $\Sigma \frac{m}{a_1}$. Next, $\Sigma \binom{a}{2}$ is the number of integers having in common with m one of the factors $a_1 a_2, a_1 a_3, \dots$, and hence equals $\Sigma \{m/(a_1 a_2)\}$. Thus

$$\phi(m) = m - \Sigma \frac{m}{a_1} + \Sigma \frac{m}{a_1 a_2} - \dots$$

R. Dedekind²⁷ gave a general theorem on the inversion of functions (to be explained in the chapter on that subject), which for the special case of $\phi(n)$ becomes a proof like Betti's. Cf. Chrystal's Algebra, II, 1889, 511; Mathews' Theory of Numbers, 1892, 5; Borel and Drach,⁸¹ p. 27.

J. B. Sturm²⁸ evaluated $\phi(N)$ by a method which will be illustrated for the case $N=15$. From $1, \dots, 15$ delete the five multiples of 3. Among the remaining ten numbers there are as many multiples of 5 as there are multiples of 5 among the first ten numbers. Hence $\phi(15) = 10 - 2 = 8$. The theorem involved is the following. From the three sets

$$1, 2, 3, * 4, 5; \quad 6, * 7, 8, 9, * 10; \quad 11, 12, * 13, 14, 15^*$$

delete (by marking with an asterisk) the multiples of 3. The numbers 11, 13, 14 which remain in the final set are congruent modulo 5 to the numbers 6, 3, 9 deleted from the earlier sets.

J. Liouville²⁹ proved by use of (4) that, for $|x| < 1$,

$$\sum_{m=1}^{\infty} \frac{\phi(m)x^m}{1-x^m} = \frac{x}{(1-x)^2}, \quad \sum_{m=1}^{\infty} \frac{\phi(m)x^m}{1-x^{2m}} = \sum_{m=1}^{\infty} \frac{\phi(m)x^m}{1+x^m} = \frac{x(1+x^2)}{(1-x^2)^2},$$

²⁶Bertrand's *Algèbre*, Ital. transl. with notes by Betti, Firenze, 1856, note 5. Proof reproduced by Fontebasso³⁴, pp. 74-77.

²⁷Jour. für Math., 54, 1857, 21. Dirichlet-Dedekind, *Zahlentheorie*, §138.

²⁸Archiv Math. Phys., 29, 1857, 448-452.

²⁹Jour. de mathématiques, (2), 2, 1857, 433-440.

where m in Σ' ranges only over the positive odd integers. The final fraction equals $x+3x^3+5x^5+\dots$. From the coefficient of x^n in the expansion of the third sum, we conclude that, if n is even,

$$\Sigma(-1)^{\delta-1}\phi(d)=0 \quad (\delta=n/d),$$

where d ranges over all the divisors of n . Let δ_1 range over the odd values of δ , and δ_2 over the even values of δ ; then

$$\Sigma\phi\left(\frac{n}{\delta_1}\right)=\Sigma\phi\left(\frac{n}{\delta_2}\right)=\frac{n}{2},$$

the value $n/2$ following from (4). Another, purely arithmetical, proof is given. Finally, by use of (4), it is proved that, if $s>2$,

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = S_{s-1}/S_s, \quad S_m = \sum_{n=1}^{\infty} \frac{1}{n^m}.$$

A. Cayley³⁰ discussed the solution for N of $\phi(N)=N'$. Set $N=a^ab^b\dots$, where a, b, \dots are distinct primes. Multiply

$$1+(a-1)\{a\}+a(a-1)\{a^2\}+\dots+a^{a-1}(a-1)\{a^a\}+\dots$$

by the analogous series in b , etc.; the bracketed terms are to be multiplied together by enclosing their product in a bracket. The general term of the product is evidently

$$\Pi a^{a-1}(a-1)\cdot\{a^ab^b\dots\}=\phi(N)\{N\}.$$

Hence in the product first mentioned each of the bracketed numbers which are multiplied by the coefficient N' will be a solution N of $\phi(N)=N'$. We need use only the primes a for which $a-1$ divides N' , and continue each series only so far as it gives a divisor of N' for the coefficient of $a^{a-1}(a-1)$.

V. A. Lebesgue³¹ proved $\phi(Z)=n\phi(z)$ as had Crelle¹⁷ and then $\phi(z)=\Pi(p_i-1)$ by the usual method of excluding multiples of p_1, \dots, p_n in turn. By the last method he proved (pp. 125-8) Legendre's (5), and the more general formula preceding (5).

J. J. Sylvester³² proved (4) by the method of Ettingshausen,⁷ using (2) instead of (3). By means of (4) he gave a simple proof of the first formula of Dirichlet;²¹ call the left member u_n ; since $[n/r]-[(n-1)/r]=1$ or 0, according as n is or is not divisible by r ,

$$u_n-u_{n-1}=\Sigma\phi(d)=n, \quad u_n=\frac{n(n+1)}{2}+c.$$

The constant c is zero since $u_1=1$. He stated the generalization

$$\sum_{i=1}^n \left\{ \phi(i^r) \left(1^{r-1} + 2^{r-1} + \dots + \left[\frac{n}{i} \right]^{r-1} \right) \right\} = 1^r + 2^r + \dots + n^r.$$

He remarked that the theorem in its simplest form is

$$n^r = \Sigma \{ \phi(i_1^{r-1}) \phi(i_2^{r-2}) \dots \phi(i_{r-1}) \cdot n / (i_1 i_2 \dots i_r) \},$$

³⁰London Ed. and Dublin Phil. Mag., (4), 14, 1857, 539-540.

³¹Exercices d'analyse numérique, 1859, 43-45.

³²Quar. Jour. Math., 3, 1860, 186-190; Coll. Math. Papers, 2, 225-8.

the example given being $r=2$, $n=4$, whence the divisors of n are 1·1, 2·1, 4·1, 1·2, 2·2, 1·4 and the above terms are

$$1 \cdot 1 \cdot 1, \quad 1 \cdot 1 \cdot 1, \quad 1 \cdot 1 \cdot 2, \quad 2 \cdot 1 \cdot 1, \quad 2 \cdot 1 \cdot 1, \quad 4 \cdot 2 \cdot 1,$$

with the sum 4^2 . [With this obscure result contrast that by Cantor.⁴⁹]

G. L. Dirichlet³³ completed by induction Euler's² method of proving (3), obtaining at the same time the generalization that, if p, q, \dots, s are divisors, relatively prime in pairs, of N , the number of integers $\leq N$ which are divisible by no one of p, \dots, s is

$$N \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \dots \left(1 - \frac{1}{s}\right).$$

A proof (§13) of (4) follows from the fact that, if d is a divisor of N , there are exactly $\phi(d)$ integers $\leq N$ having with N the g. c. d. N/d .

P. A. Fontebasso³⁴ repeated the last remark and gave Gauss' proof of (1).

E. Laguerre³⁵ employed any real number k and integer m and wrote $(m, m/k)$ for the number of integers $\leq m/k$ which are prime to m . By continuous variation of k he proved that

$$\Sigma(d, d/k) = [m/k],$$

where d ranges over the divisors of m . For $k=1$, this reduces to (4).

F. Mertens³⁶ obtained an asymptotic value for $\phi(1) + \dots + \phi(G)$ for G large. He employed the function $\mu(n)$ [see Ch. XIX] and proved that

$$\sum_{m=1}^G \phi(m) = \frac{1}{2} \sum_{n=1}^G \mu(n) \left\{ \left[\frac{G}{n} \right]^2 + \left[\frac{G}{n} \right] \right\} = \frac{3}{\pi^2} G^2 + \Delta$$

$$|\Delta| < G \left(\frac{1}{2} \log_e G + \frac{1}{2} C + \frac{5}{8} \right) + 1,$$

where C is Euler's constant 0.57721... This upper limit for Δ is more exact than that by Dirichlet.²¹

T. Pepin³⁷ stated that, if $n = a^\alpha b^\beta \dots$ (a, b, \dots distinct primes),

$$n = \phi(n) + \Sigma a^{\alpha-1} \phi \left(\frac{n}{a^\alpha} \right) + \Sigma a^{\alpha-1} b^{\beta-1} \phi \left(\frac{n}{a^\alpha b^\beta} \right) + \dots + a^{\alpha-1} b^{\beta-1} \dots$$

Moret-Blanc³⁸ proved the latter by noting that the first sum is the number of integers $< n$ which are divisible by a single one of the primes a, b, \dots , the second sum is the number of integers $< n$ divisible by two of the primes, \dots , while $a^{\alpha-1} b^{\beta-1} \dots$ is the number of integers $< n$ divisible by all those primes.

H. J. S. Smith³⁹ considered the m -rowed determinant Δ_m having as the element in the i th row and j th column the g. c. d. (i, j) of i, j . Let $l_1 = m$,

³³Zahlentheorie, §11, 1863; ed. 2, 1871; ed. 3, 1879; ed. 4, 1894.

³⁴Saggio di una introd. all'arit. trascendente, Treviso, 1867, 23-26.

³⁵Bull. Soc. Math. France, 1, 1872-3, 77.

³⁶Jour. für Math., 77, 1874, 289-91.

³⁷Nouv. Ann. Math., (2), 14, 1875, 276.

³⁸*Ibid.*, p. 374. L. Gegenbauer, Monatsh. Math. Phys., 4, 1893, 184, gave a generalization to primary complex numbers.

³⁹Proc. London Math. Soc., 7, 1875-6, 208-212; Coll. Papers, 2, 161.

l_2, l_3, \dots be those divisors of $m = p^a q^b \dots t^r$ which are given by the expansion of the product

$$\phi(m) = (p^a - p^{a-1}) \dots (t^r - t^{r-1}) = l_1 - l_2 + l_3 - \dots - l_s.$$

It is proved that

$$\phi(m, k) \equiv (l_1, k) - (l_2, k) + \dots - (l_s, k)$$

[called Smith's function by Lucas,⁷² p. 407] is zero if $k < m$, but equals $\phi(m)$ if $k = m$. Hence if to the m th column of Δ_m we add the columns with indices l_3, l_5, \dots and subtract the columns with indices l_2, l_4, \dots , we obtain an equal determinant in which the elements of the m th column are zero with the exception of the element $\phi(m)$. Hence $\Delta_m = \Delta_{m-1} \phi(m)$, so that

$$(6) \quad \Delta_m = \phi(1) \phi(2) \dots \phi(m).$$

If we replace the element $\delta = (i, j)$ by any function $f(\delta)$ of δ , we obtain a determinant equal to $F(1) \dots F(m)$, where

$$F(m) = f(m) - \sum f\left(\frac{m}{p}\right) + \sum f\left(\frac{m}{pq}\right) - \dots$$

Particular cases are noted. For $f(\delta) = \delta^k$, $F(m)$ becomes Jordan's²⁰⁰ function $J_k(m)$. Next, if $f(\delta)$ is the sum of the k th powers of the divisors of δ , then $F(m) = m^k$. Finally, if $f(\delta) = 1^k + 2^k + \dots + \delta^k$, it is stated erroneously that $F(m)$ is the sum $\phi_k(m)$ of the k th powers of the integers $\leq m$ and prime to m . [Smith overlooked the factors $a^k, a^k b^k, \dots$ in Thacker's¹⁵⁰ first expression for $\phi_k(n)$, which is otherwise of the desired form $F(n)$. The determinant is not equal to $\phi_k(1) \dots \phi_k(m)$, as the simple case $k = 1, m = 2$, shows.]

In the main theorem we may replace $1, \dots, m$ by any set of distinct numbers μ_1, \dots, μ_m such that every divisor of each μ_i is a number of the set; the determinant whose element in the i th row and j th column is $f(\delta)$, where $\delta = (\mu_i, \mu_j)$, equals $F(\mu_1) \dots F(\mu_m)$. Examples of sets of μ 's are the numbers in their natural order with the multiples of given primes rejected; the numbers composed of given primes; and the numbers without square factors.

R. Dedekind⁴⁰ proved that, if n be decomposed in every way into a product ad , and if e is the g. c. d. of a, d , then

$$\sum_e^a \phi(e) = n \Pi \left(1 + \frac{1}{p} \right),$$

where a ranges over all divisors of n , and p over the prime divisors of n .

P. Mansion⁴¹ stated that Smith's relation (6) yields a true relation if we replace the elements $1, 2, \dots$ of the determinant Δ_m by any symbols x_1, x_2, \dots , and replace $\phi(m)$ by $x_1 - x_2 + x_3 - \dots$. [But the latter is only another form of Smith's $F(m)$ when we write x_δ for Smith's $f(\delta)$, so that the generalization is the same as Smith's.]

⁴⁰Jour. für Math., 83, 1877, 288. Cf. H. Weber, Elliptische Functionen, 1891, 244-5; ed. 2, 1908 (Algebra III), 234-5.

⁴¹Messenger Math., 7, 1877-8, 81-2.

P. Mansion⁴² proved (6), showing that $\phi(m, k)$ equals $\phi(m)$ or 0, according as m is or is not a divisor of k . [Cf. Bachmann, *Niedere Zahlentheorie*, I, 1902, 97–8.] He repeated his⁴¹ “generalization.” He stated that if a and b are relatively prime, the products of the $\phi(a)$ numbers $< a$ and prime to a by the numbers $< b$ and prime to b give the numbers $< ab$ and prime to ab [false for $a=4, b=3$; cf. Mansion⁴⁴]. His proof of (4) should have been credited to Catalan.¹¹

E. Catalan⁴³ gave a condensation and slight modification of Mansion’s⁴² paper. C. Le Paige (*ibid.*, pp. 176–8) proved Mansion’s⁴⁴ theorem that every product equals a determinant formed from the factors.

P. Mansion⁴⁴ proved that the determinant $|c_{ij}|$ of order n equals $x_1 x_2 \dots x_n$ if $c_{ij} = \sum x_p$, where p ranges over the divisors of the g. c. d. of i, j . To obtain a “generalization” of Smith’s theorem, set $z_1 = x_1, z_2 = x_1 + x_2, \dots, z_i = \sum x_d$, where d ranges over all the divisors of i . Solving, we get

$$x_m = z_m - z_{l_1} + z_{l_2} - \dots,$$

where the l ’s are defined above.³⁹ Thus each c_{ij} is a z . For example, if $n=4$,

$$|c_{ij}| = \begin{vmatrix} z_1 & z_1 & z_1 & z_1 \\ z_1 & z_2 & z_1 & z_2 \\ z_1 & z_1 & z_3 & z_1 \\ z_1 & z_2 & z_1 & z_4 \end{vmatrix}.$$

For $z_i = i, x_i$ becomes $\phi(i)$ and we get (6). [As explained in connection with Mansion’s⁴¹ first paper, the generalization is due to Smith.]

J. J. Sylvester⁴⁵ called $\phi(n)$ the totient $\tau(n)$ of n , and defined the totitives of n to be the integers $< n$ and prime to n .

F. de Rocquigny⁴⁶ stated that, if $\phi^2(N)$ denotes $\phi\{\phi(N)\}$, etc.,

$$\phi^p(N^m) = \phi^{p-2}(N^{m-2}) \cdot \phi^{p-1}\{(N-1)^2\},$$

if N is a prime and $m > 2, p > 2$. He stated incorrectly (*ibid.*, 50, 1879, 604) that the number of integers $\leq P$ which are prime to $N = a^a b^b \dots$ is $P(1-1/a)(1-1/b) \dots$.

A. Minine⁴⁷ noted that the last result is correct for the case in which P is divisible by each prime factor a, b, \dots of N . He wrote symbolically $nE\frac{(1)}{x}$ for $[n/x]$, the greatest integer $\leq n/x$. By deleting from $1, \dots, P$ the $[P/a]$ numbers divisible by a , then the multiples of b , etc., we obtain for the number of integers $\leq P$ which are prime to N the expression

$$\phi(N)_P = P \left\{ 1 - E\frac{(1)}{a} \right\} \left\{ 1 - E\frac{(1)}{b} \right\} \dots$$

[equivalent to (5)]. If N, N', N'', \dots are relatively prime by twos,

⁴²Annales de la Soc. Sc., Bruxelles, 2, II, 1877–8, 211–224. Reprinted in Mansion’s *Sur la théorie des nombres*, Gand, 1878, §3, pp. 3–16.

⁴³Nouv. Corresp. Math., 4, 1878, 103–112.

⁴⁴Bull. Acad. R. Sc. de Belgique, (2), 46, 1878, 892–9.

⁴⁵Amer. Jour. Math., 2, 1879, 361, 378; Coll. Papers, 3, 321, 337. Nature, 37, 1888, 152–3.

⁴⁶Les Mondes, Revue Hebdom. des Sciences, 48, 1879, 327.

⁴⁷Ibid., 51, 1880, 333. Math. Soc. of Moscow, 1880. Jour. de math. élém. et spéc., 1880, 278.

$$\phi(N)_P \cdot \phi(N')_{P'} \cdot \phi(N'')_{P''} \dots = \phi(NN'N'' \dots)_P \cdot P'P'' \dots$$

E. Lucas⁴⁸ stated and Radicke proved that

$$\sum_{a=1}^n \psi(a, n) = \sum_{k=2}^n \phi(k), \quad \sum_{a=1}^{n-1} a\psi(a, n) = \frac{1}{2} \sum_{k=2}^n k\phi(k),$$

if $\psi(a, n)$ is the number of integers $> a$, prime to a and $\leq n$.

H. G. Cantor⁴⁹ proved by use of ζ -functions that

$$\sum \nu_0^{\rho-1} \nu_1^{\rho-2} \dots \nu_{\rho-2}^1 \phi(\nu_0) \phi(\nu_1) \dots \phi(\nu_{\rho-1}) = n^\rho,$$

summed for all distinct sets of positive integral solutions $\nu_0, \dots, \nu_{\rho-1}$ of $\nu_0 \dots \nu_{\rho-1} = n$, and noted that this result can be derived from the special case (4).

O. H. Mitchell⁵⁰ defined the a -totient $\tau_a(k)$ of $k = a^t b^u \dots$ (where a, b, \dots are distinct primes) to be the number of integers $< k$ which are divisible by a , but by no one of the remaining prime factors b, c, \dots of k . Similarly, the ab -totient $\tau_{ab}(k)$ of k is the number of integers $< k$ which are divisible by a and b , but not by c, \dots ; etc. If $k = a^t b^u c^v$,

$$\begin{aligned} \tau_a(k) &= a^{t-1} \phi(b^u c^v), & \tau_{ab}(k) &= a^{t-1} b^{u-1} \phi(c^v), & \tau_{abc}(k) &= a^{t-1} b^{u-1} c^{v-1}, \\ \phi(k) + \sum_3 \tau_a(k) + \sum_3 \tau_{ab}(k) + \tau_{abc}(k) &= k. \end{aligned}$$

If σ contains the same primes as s , but with the same exponents as in k , so that $\sigma = a^t$ if $s = a$, it is stated (p. 302) that

$$\tau_s(k) = \frac{\sigma}{s} \phi\left(\frac{k}{\sigma}\right).$$

C. Crone⁵¹ evaluated $\phi(n)$ by an argument valid only when n is a product of distinct primes p_1, \dots, p_q . The number of integers $< n$ having a factor in common with n is then

$$A = \sum \left(\frac{n}{p_1} - 1 \right) - \sum \left(\frac{n}{p_1 p_2} - 1 \right) + \dots + (-1)^q \sum \left(\frac{n}{p_1 \dots p_{q-1}} - 1 \right).$$

The sum of the second terms of each sum is

$$-\left(\frac{q}{1}\right) + \left(\frac{q}{2}\right) - \dots - (-1)^q \left(\frac{q}{q-1}\right) = -1 - (-1)^q.$$

Hence the number of integers $< n$ and prime to n is

$$\begin{aligned} n-1-A &= n - \sum \frac{n}{p_1} + \sum \frac{n}{p_1 p_2} - \dots - (-1)^q \sum \frac{n}{p_1 \dots p_{q-1}} + (-1)^q \\ &= n \left(1 - \frac{1}{p_1} \right) \dots \left(1 - \frac{1}{p_q} \right), \end{aligned}$$

provided $n = p_1 \dots p_q$. [To modify the proof to make it valid for any n , we need only add to A the term

$$-(-1)^q \left(\frac{n}{p_1 \dots p_q} - 1 \right)$$

and hence replace $(-1)^q$ by $(-1)^q n / (p_1 \dots p_q)$ in $n-1-A$.]

⁴⁸Nouv. Corresp. Math., 6, 1880, 267-9. Also Lucas,⁷² p. 403.

⁴⁹Göttingen Nachrichten, 1880, 161; Math. Ann., 16, 1880, 583-8.

⁵⁰Amer. Jour. Math., 3, 1880, 294.

⁵¹Tidsskrift for Matematik, (4), 4, 1880, 158-9.

Franz Walla⁵² considered the product P of the first n primes > 1 . Let x_1, \dots, x_ν be the integers $< P/2$ and prime to P , so that $\nu = \phi(P)/2$. Then, if $n > 2$, half of the x 's are $\equiv 1 \pmod{4}$ and the others are $\equiv 3 \pmod{4}$. Also, the absolute values of $\frac{1}{2}P - 2x_j$ ($j = 1, \dots, \nu$) are the x 's in some order. Half of the x 's are $< P/4$.

J. Perott⁵³ proved that

$$\Phi(N) \equiv \sum_{h=1}^N \phi(h) = \frac{1}{2} + \frac{1}{2} \{ N^2 - \sum \left[\frac{N}{p_i} \right]^2 + \sum \left[\frac{N}{p_i p_j} \right]^2 - \dots \},$$

the context showing that the summations extend over all the primes p_i for which $1 < p_i \leq N$ [Lucas⁷²]. He proved that

$$\lim_{N=\infty} \frac{\Phi(N)}{N^2} = \frac{3}{\pi^2}$$

and gave a table showing the approximation of $3N^2/\pi^2$ to $\Phi(N)$ for $N \leq 100$. The last formula, proved earlier by Dirichlet²¹ and Mertens,³⁶ was proved by G. H. Halphen⁵⁴ by the use of integrals and ζ -functions.

Sylvester^{54a} defined the frequency δ of a divisor d of one or more given integers a, b, \dots, l to be the number of the latter which are divisible by d . By use of (4) he proved the generalization

$$\sum_d \delta \phi(d) = a + b + \dots + l.$$

J. J. Sylvester⁵⁵ stated that the number of [irreducible proper] fractions whose numerator and denominator are $\leq j$ is $T(j) = \phi(1) + \dots + \phi(j)$, and that

$$\sum_{k=1}^j T\left[\frac{j}{k}\right] \equiv \sum_{k=1}^j \sum_{i=1}^{[j/k]} \phi(i) = \frac{j^2 + j}{2},$$

whence $T(j)/j^2$ approximates $3/\pi^2$ as j increases indefinitely.

If $u(x)$ denotes the sum of all the integers $< x$ and prime to x , and if $U(j) = u(1) + \dots + u(j)$, then $U(j)$ is the sum of the numerators in the above set of fractions, and*

$$\sum_{k=1}^j k U\left[\frac{j}{k}\right] = \frac{1}{6}j(j+1)(j+2).$$

When j increases indefinitely, $U(j)/j^3$ approximates $1/\pi^2$. For each integer $n \leq 1000$ the values of $\phi(n)$, $T(n)$, $3n^2/\pi^2$ are tabulated.

Sylvester⁵⁶ stated the preceding results and noted that the first formula is equivalent to

$$\sum_{r=1}^{\infty} \left[\frac{j}{r} \right] \phi(r) = \frac{1}{2}(j^2 + j).$$

⁵²Archiv Math. Phys., 66, 1881, 353-7.

⁵³Bull. des Sc. Math. et Astr., (2), 5, I, 1881, 37-40.

⁵⁴Comptes Rendus Paris, 96, 1883, 634-7.

^{54a}Amer. Jour. Math., 5, 1882, 124; Coll. Math. Papers, 3, 611.

⁵⁵Phil. Mag., 15, 1883, 251-7; 16, 1883, 230-3; Coll. Math. Papers, 4, 101-9. Cf. Sylvester.⁵⁴

⁵⁶Comptes Rendus Paris, 96, 1883, 409-13, 463-5; Coll. Math. Papers, 4, 84-90. Proofs by F. Rogel and H. W. Curjel, Math. Quest. Educ. Times, 66, 1897, 62-4; 70, 1899, 56.

*With denominator 3, but corrected to 6 by Sylvester,⁵⁶ which accords with Cesàro.⁶⁵ The editor of Sylvester's Papers stated in both places that the second member should be $j(j+1)(2j+1)/12$, evidently wrong for $j=2$.

E. Cesàro⁵⁷ proved that, if f is any function,

$$\sum_{n=1}^{\infty} \frac{x^n f(n)}{1-x^n} = \sum_{n=1}^{\infty} x^n F(n), \quad F(n) \equiv \sum f(d),$$

where d ranges over the divisors of n . For $f = \phi$, we have $F(x) = x$ and obtain Liouville's²⁹ first formula. By the same specialization (p. 64) of another formula (given in Chapter X on sums of divisors⁶¹), Cesàro derived the final formula of Liouville.²⁹ If (n, j) is the g. c. d. of n and j , then (p. 77, p. 80)

$$\sum_{j=1}^n (n, j) = \sum d \phi\left(\frac{n}{d}\right), \quad \sum \frac{1}{(n, j)} = \frac{1}{n} \sum d \phi(d), \quad \sum \phi(n, j) = \sum \phi(d) \phi\left(\frac{n}{d}\right).$$

If (p. 94) p is one of the integers $a, \beta, \dots \leq n$ and prime to n ,

$$\sum g(a) F(a) = \sum G(a) f(a), \quad F(x) \equiv \sum f(d), \quad G(p) \equiv \sum g(pa),$$

where d ranges over the divisors of x . For $g(x) = 1$, this gives

$$\sum f(a) \phi(n, n/a) = \sum F(a),$$

where (p. 96) $\phi(n, x)$ is the number of integers $\leq x$ and prime to n . Cesàro (pp. 144–151, 302–3) discussed and modified Perott's⁵³ proof of his first formula, criticizing his replacement of $[n/k]$ by n/k for n large. He gave (pp. 153–6) a simple proof that the mean⁶⁷ of $\phi(n)$ is $6n/\pi^2$ and reproduced the proofs by Dirichlet²¹ and Mertens,³⁶ the last essentially the same as Perott's. For $\zeta(m) = 1 + 1/2^m + 1/3^m + \dots$,

$$\sum \frac{1}{a^m} (m > 1), \quad \sum \frac{1}{a}, \quad \sum \frac{1}{a^m \phi(a)} (m > 1), \quad \sum \frac{1}{\phi(a)}$$

equal asymptotically (pp. 167–9)

$$\zeta(m)/\zeta(m+1), \quad (6 \log n)/\pi^2, \quad \zeta(m+1), \quad \log n.$$

As a corollary (p. 251) to Mansion's⁴¹ generalization of Smith's theorem we have the result that the determinant of order n^2 , each element being 1 or 0 according as the g. c. d. of its two indices is or is not a perfect square, equals $(-1)^{a+b+\dots}$, where $p^a q^b \dots$ is the value of $n!$ expressed in terms of its prime factors.

Cesàro⁵⁸ considered any function $F(x, y)$ of the g. c. d. of x, y , and the determinant Δ_n of order n having the element $F(u_i, u_j)$ in the i th row and j th column, where u_1, \dots, u_n are integers in ascending order such that each divisor of every u_i is a u . Employing the function $\mu(n)$ [see Ch. XIX], he noted that

$$\sum_{i=1}^n \mu\left(\frac{u_n}{u_i}\right) F(u_r, u_i) = f(u_n) \text{ or } 0,$$

⁵⁷Mém. Soc. R. Sc. de Liège, (2), 10, 1883, No. 6, 74.

⁵⁸Atti Reale Accad. Lincei, (4), 1, 1884–5, 709–711.

according as u_r is or is not divisible by u_n , while

$$f(x) = \mu(x)F(1) + \mu\left(\frac{x}{2}\right)F(2) + \mu\left(\frac{x}{3}\right)F(3) + \dots$$

Hence if we multiply the elements of the i th column of Δ_n by $\mu(u_n/u_i)$ and add the products to the last column for $i = 1, \dots, n-1$, the new elements of the last column are zero except the final element, which is $f(u_n)$. Thus

$$\Delta_n = f(u_n)\Delta_{n-1} = f(u_1)f(u_2) \dots f(u_n).$$

[These results are due to Smith,³⁹ not merely the case $u_i = i$ as stated.]

Cesàro⁵⁹ noted that $|u_{ij}| = f(1) \dots f(n)$ if

$$u_{ij} = \sum_{\nu=1}^n f(\nu) h\left(\frac{i}{\nu}\right) h_1\left(\frac{j}{\nu}\right),$$

where the function h has the property that the determinant with the general element $h(i/j)$ is unity, and similarly for h_1 .

Cesàro⁶⁰ gave the last result for the case in which $h(x) = h_1(x) = 1$ or 0 according as x is or is not an integer. P. Mansion (p. 250) stated that he⁴⁴ had employed a similar proof.

Cesàro⁶¹ duplicated his paper⁵⁸ and transformed its final result into

$$\left| \frac{1}{F[i, j]} \right|_n = \frac{f(1)f(2) \dots f(n)}{F^2(n!)},$$

where $[i, j] = ij/(i, j)$ is the l. c. m. of i, j , and $F(x)$ is a function such that $F(xy) = F(x)F(y)$. In particular, if $F(x) = 1/x$, then $f(x) = \phi(x)\pi(x)/x^2$, where $\pi(n)$ is the product of the negatives of the distinct prime factors of n . Hence

$$|[i, j]|_n = \phi(1) \dots \phi(n)\pi(1) \dots \pi(n).$$

Cesàro⁶² investigated the r -rowed minors of the n -rowed determinant whose general element is $F(\delta) = F(i, j)$, where δ is the g. c. d. of i, j . It is shown that the $(n-\nu)$ -rowed determinant whose general element is $F(i+\nu, j+\nu)$ is equal to the sum of certain products of $f(1), \dots, f(n)$ taken $n-\nu$ at a time, the case $\nu=0$ being Smith's theorem. Here

$$f(x) = \sum_j \mu\left(\frac{x}{j}\right) F(j), \quad F(x) = \sum f(d) \quad (d \text{ divisor of } x).$$

Cesàro⁶³ stated that the $(n-1)$ -rowed determinant, whose general element u_{ij} equals the number of divisors common to $i+1$ and $j+1$, equals the number of integers $\leq n$ deprived of square factors > 1 .

³⁹Atti. Reale Accad. Lincei, (4), 1, 1884-5, 711-5.

⁶⁰Mathesis, 5, 1885, 248-9.

⁶¹Giornale di Mat., 23, 1885, 182-197.

⁶²Annales de l'école normale sup., (3), 2, 1885, 425-435.

⁶³Nouv. Ann. Math., (3), 4, 1885, 56.

Cesàro⁶⁴ employed $F(n) = \Sigma f(d)$, $G(n) = \Sigma g(d)$, where d ranges over the divisors of n , and proved that

$$\begin{vmatrix} 0 & G(1) & G(2) & \dots & G(n) \\ G(1) & F(1, 1) & F(1, 2) & \dots & F(1, n) \\ \dots & \dots & \dots & \dots & \dots \\ G(n) & F(n, 1) & F(n, 2) & \dots & F(n, n) \end{vmatrix} = -f(1) \dots f(n) \sum_{\nu=1}^n \frac{g^2(\nu)}{f(\nu)}.$$

In particular, if $F(n)$ is the number of divisors of n and if $G(n)$ is the number of prime divisors of n , the determinant, apart from signs, equals the number of primes $\leq n$.

E. Cesàro⁶⁵ wrote (a, b) for the g. c. d. of a, b . If $F(n) = \Sigma f(d)$, where d ranges over the divisors of n , then

$$\sum_{i=1}^N F \{ (n, i) \} = \Sigma f(d) N/d.$$

In particular, if $I_\epsilon(n)$ is the number of irreducible fractions $\leq \epsilon$ of denominator n ,

$$I_\epsilon(n) = \Sigma \left[\frac{n\epsilon}{d} \right] \mu(d), \quad \Sigma I_\epsilon(d) = [n\epsilon].$$

The last formula, due to Laguerre,³⁵ follows by inversion (Ch. XIX), and directly from the fact that $I_\epsilon(d)$ is the number of the first $[n\epsilon]$ integers which with n have the g. c. d. n/d . The number of irreducible fractions $\leq \epsilon$ of denominator $\leq n$ is $\Phi_\epsilon(n) = I_\epsilon(1) + \dots + I_\epsilon(n)$. We have

$$\Phi_\epsilon(n) = \sum_{j=1}^{\infty} \mu(j) \sum_{i=1}^{[n/j]} [i\epsilon], \quad \lim_{n=\infty} \Phi_\epsilon(n)/n^2 = \frac{3\epsilon}{\pi^2} \quad (\epsilon > 0),$$

due to Sylvester⁵⁵ for $\epsilon = 1$. Let $\phi_\epsilon^{(\nu)}(n)$ be the sum of the ν th powers of the numerators of the irreducible fractions $\leq \epsilon$ of denominator n . Set

$$\Phi_\epsilon^{(\nu)}(n) = \sum_{i=1}^n \phi_\epsilon^{(\nu)}(i), \quad s_\nu(n) = \sum_{i=1}^n i^\nu.$$

Then

$$\sum_{i=1}^n i^\nu \Phi_\epsilon^{(\nu)} \left[\frac{n}{i} \right] = \sum_{i=1}^n s_\nu [i\epsilon],$$

which generalizes the two formulas of Sylvester.⁵⁵ Also,

$$\Phi_\epsilon^{(\nu)}(n) = \frac{6}{\pi^2} \cdot \frac{\epsilon^{\nu+1}}{\nu+1} \cdot \frac{n^{\nu+2}}{\nu+2}, \text{ asymptotically.}$$

Cesàro^{65a} factored determinants of the type in his paper,⁵⁸ the function F now being such that $F(xy)/\{F(x)F(y)\}$ is a function of the g. c. d. of x, y .

L. Gegenbauer^{65b} gave a complicated theorem involving several general functions, special cases of which give Sylvester's⁵⁵ two summation formulas.

⁶⁴Nouv. Ann. Math., (3), 5, 1886, 44-47.

⁶⁵Annali di Mat., (2), 14, 1886-7, 143-6.

^{65a}Giornale di Mat., 25, 1887, 18-19.

^{65b}Sitzungsber. Ak. Wiss. Wien (Math.), 94, 1886, II, 757-762.

P. S. Poretzky⁶⁶ gave a formula for the function $\psi(m)$ whose values are the $\phi(m)$ integers $< m$ and prime to m . For the case $m = 2 \cdot 3 \cdot 5 \dots p$, where p is a prime,

$$\psi(m) = m \left\{ \sum_{p_i=2}^p \frac{\psi(p_i)}{p_i} - K \right\},$$

where K is an integer. Application is made to the finding of a prime exceeding a given number, and to a generalization of the sieve of Eratosthenes.

E. Cesàro⁶⁷ gave a very simple proof of the known fact that

$$\lim_{n \rightarrow \infty} \frac{\phi(1) + \dots + \phi(n)}{n^2} = \frac{3}{\pi^2},$$

which he expressed in words by saying that $\phi(n)$ is asymptotic to $6n/\pi^2$ (not meaning that the limit of $\phi(n)/n$ is $6/\pi^2$). On the distinction between asymptotic mean and median value, see *Encyclopédie des sc. math.*, I, 17 (vol. 3), p. 347.

Cesàro⁶⁸ noted that if $F(i, j)$ is a function of the g. c. d. of i, j , then $Q = \sum F(i, j) x_i x_j$ ($i, j = 1, \dots, n$) becomes $q = \sum f(i) y_i^2$ by the substitution $y_k = x_k + x_{2k} + x_{3k} + \dots$, provided $F(n) = \sum f(d)$, d ranging over the divisors of n . Since the determinant of the substitution is unity, the discriminants of Q and q are equal. Hence we have the theorem of Smith.³⁹ A generalization is obtained by use of $\sum F(\epsilon_i, \epsilon_j) x_i x_j$, where the numbers $\epsilon_1, \epsilon_2, \dots$ include the divisors of each ϵ .

E. Catalan⁶⁹ proved that, if d ranges over the divisors of $N = a^\alpha b^\beta \dots$,

$$\sum \frac{\phi(d)}{d} = \Pi \left\{ 1 + \frac{a(a-1)}{a} \right\}, \quad \sum \frac{d}{\phi(d)} = \Pi \left(1 + \frac{aa}{a-1} \right).$$

E. Busche⁷⁰ derived at once from Dirichlet's²¹ formula the result

$$\sum_{x=1}^{\infty} \phi(x) \left\{ \rho \left(\frac{n}{x} \right) + \rho \left(\frac{n'}{x} \right) + \dots \right\} = \sum n n',$$

where $\rho(a) = a - [a]$. The case $n = n' = n'' = \dots$ leads to

$$\sum \phi(x) = (\nu - 1)n^2,$$

where x takes all values for which $\rho(n/x) > \rho(\nu n/x)$. If we take $n = 1$ and add $\phi(1) = 1$, we get (4) for $N = \nu$. Next, $\sum \phi(x) = r r' \delta^2$, where x takes all values for which

$$\frac{y + y' - 1}{r + r'} \leq \rho \left(\frac{\delta}{x} \right) < \frac{y}{r}, \frac{y'}{r'} \quad (y = 1, \dots, r; y' = 1, \dots, r').$$

⁶⁶Math. phys. soc. Kasan, 6, 1888, 52-142 (in Russian).

⁶⁷Comptes Rendus Paris, 106, 1888, 1651; 107, 1888, 81, 426; Annali di Mat., (2), 16, 1888-9, 178 (discussion with Jensen on terminology).

⁶⁸Atti Reale Accad. Lincei, Rendiconti, 2, 1888, II, 56-61.

⁶⁹Mém. Soc. Sc. Liège, (2), 15, 1888, No. 1, pp. 21-22; Mélanges Math., III, No. 222, dated 1882.

⁷⁰Math. Annalen, 31, 1888, 70-74.

For $\delta = n$, $r' = 1$, $r = \nu - 1$, this becomes the former result; for $r = r' = 1$, $\delta = n$, it becomes $\sum \phi(x) = n^2$, where x takes the values for which $\rho(n/x) \geq 1/2$.

H. W. Lloyd Tanner⁷¹ studied the group G of the totitives of n (the integers $< n$ and prime to n), finding all its subgroups and the simple groups whose direct product is G .

E. Lucas⁷² proved that, in an arithmetical progression of n terms whose common difference is prime to n , there are $\phi(d)$ terms having with n the g. c. d. n/d . If, when d ranges over the divisors of n , $\sum \psi(d) = n$ for every integer n , then (p. 401) $\psi(n) = \phi(n)$, as proved by using $n = 1, a, a^2, \dots$, and $n = ab, a^2b, \dots$, where a, b, \dots are distinct primes. He gave (pp. 500-1) a proof of Perott's⁵³ first formula by induction from $N-1$ to N , communicated to him by J. Hammond. The name "indicateur" of n is given (preface, xv) to $\phi(n)$ [Prouhet¹⁸].

C. Moreau (cf. Lucas,⁷² 501-3) considered the $C(n)$ circular permutations of n objects of which α are alike, β alike, \dots , λ alike. Thus, if $\alpha = 2, \beta = 4$, the $C(6) = 3$ distinct circular permutations are $aabbbb, ababbb, abbabb$. In general,

$$C(n) = \frac{1}{n} \sum \phi(d) \frac{(n/d)!}{(\alpha/d)! \dots (\lambda/d)!},$$

where d ranges over the divisors of the g. c. d. of $\alpha, \beta, \dots, \lambda$. In the example, $d = 1$ or 2 , and the terms of the sum are 15 and 3 .

P. A. MacMahon⁷³ noted that $C(n) = 1$ if $n = \alpha$, so that we have formula (4). His expression for the number of circular permutations of p things n at a time is quoted in Chapter III on Fermat's theorem.

A. Berger^{73a} evaluated $\sum_{k=1}^{k=n} k^{a-2} \phi(k)$. For $a = 2$ the result is $3n^2/\pi^2 + \lambda n \log n$, where λ is finite for all values of n .

E. Jablonski⁷⁴ considered rectilinear permutations of indices α, \dots, λ , with the g. c. d. D . Set $\alpha = \alpha'D, \dots, \lambda = \lambda'D, \alpha + \dots + \lambda = m = m'D$. Then the number of complete rectilinear permutations of indices $\alpha'n, \dots, \lambda'n$ is

$$P(n) = \frac{(m'n)!}{(\alpha'n)! \dots (\lambda'n)!}.$$

The number of complete circular permutations is

$$\frac{1}{m} \sum \phi(d) P\left(\frac{D}{d}\right),$$

where d ranges over the divisors of D . If $Q(D/d)$ is the number of rectilinear permutations of indices α, \dots, λ which can be decomposed into d identical portions, $\sum Q(D/d) = P(D)$. Also

⁷¹Proc. London Math. Soc., 20, 1888-9, 63-83.

⁷²Théorie des nombres, 1891, 396-7. The first theorem was proved also by U. Concina, II Boll. di Matematica, 1913, 9.

⁷³Proc. London Math. Soc., 23, 1891-2, 305-313.

^{73a}Nova Acta Regiae Soc. Sc. Upsaliensis, (3), 14, 1891, No. 2, 113.

⁷⁴Comptes Rendus Paris, 114, 1892, 904-7; Jour. de Math., (4), 8, 1892, 331-349. He proved Moreau's⁷² formula for $C(n)$.

$$\Sigma Q\left(\frac{D}{d}\right)d^t = \Sigma P\left(\frac{D}{d}\right)J_t(d),$$

where $J_t(d)$ is Jordan's²⁰⁰ function.

S. Schatunowsky⁷⁶ proved that 30 is the largest number such that all smaller numbers relatively prime to it are primes. He employed Tchebychef's²⁶¹ theorem of Ch. XVIII that, if $a > 1$, there exists at least one prime between a and $2a$. Cf. Wolfskehl,⁹¹ Landau,^{92, 113} Maillet,⁹³ Bonse,¹⁰⁶ Remak.¹¹²

E. W. Davis⁷⁶ used points with integral coordinates ≥ 0 to visualize and prove (1) and (4).

K. Zsigmondy⁷⁷ wrote r_s for the greatest integer $\leq r/s$ and proved that, if a takes those positive integral values $\leq r$ which are divisible by no one of the given positive integers n_1, \dots, n_p which are relatively prime in pairs,

$$\Sigma f(a) = \sum_{k=1}^r f(k) - \sum_n \sum_{k=1}^{r_n} f(kn) + \sum_{n, n'} \sum_{k=1}^{r_{nn'}} f(knn') - \dots,$$

n, n', \dots ranging over the combinations of n_1, \dots, n_p taken 1, 2, \dots at a time. Taking $f(k) = 1$, we obtain for the number $\phi(r; n_1, \dots, n_p)$ of integers $\leq r$, which are divisible by no one of n_1, \dots, n_p , the expression (5) obtained by Legendre for the case in which the n 's are all primes. By induction from ρ to $\rho+1$, we get

$$\begin{aligned} \phi(r; n_1, \dots, n_p, \nu_1, \dots, \nu_p) &= \phi(r; n_1, \dots, n_p) - \sum_c \phi(r_c; n_1, \dots, n_p) \\ &\quad + \sum_{r, \nu'} \phi(r_{\nu'}; n_1, \dots, n_p) - \dots, \\ r &= \phi(r; n_1, \dots, n_p) + \sum_{i=1}^p \phi(r_{n_i}; n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_p) \\ &\quad + \sum_{n, n'} \phi(r_{nn'}; n_i's \neq n, n') + \dots, \\ r &= \sum_c \phi(r_c; n_1, \dots, n_p), \end{aligned}$$

where c ranges over all combinations of powers $\leq r$ of the n 's. The last becomes (4) when n_1, \dots, n_p are the different primes dividing r . These formulas for r were deduced by him in 1896 as special cases of his inversion formula (see Ch. XIX).

J. E. Steggall⁷⁸ evaluated $\phi(n)$ by the second method of Crelle.¹⁷

P. Bachmann⁷⁹ gave an exposition of the work of Dirichlet,²¹ Mertens,³⁶ Halphen⁵⁴ and Sylvester⁵⁵ on the mean of $\phi(n)$, and (p. 319) a proof of (5).

L. Goldschmidt⁸⁰ gave an evaluation of $\phi(n)$ by successive steps which may be combined as follows. Let p be a prime not dividing k . Each of

⁷⁶Spaczkinski Bote (phys. math.), 14, 1893, No. 159, p. 65; 15, 1893, No. 180, pp. 276-8 (Russian).

⁷⁷Amer. Jour. Math., 15, 1893, 84.

⁷⁸Jour. für Math., 111, 1893, 344-6.

⁷⁹Proc. Edinburgh Math. Soc., 12, 1893-4, 23-24.

⁸⁰Die Analytische Zahlentheorie, 1894, 422-430, 481-4.

⁸¹Zeitschrift Math. Phys., 39, 1894, 203-4.

the $\phi(k)$ integers $\leq k$ and prime to k occurs just once among the residues modulo k of the integers from lk to $(l+1)k$; taking $l=0, 1, \dots, p-1$, we obtain this residue p times. Hence there are $p\phi(k)$ numbers $\leq pk$ and prime to k . These include $\phi(k)$ multiples of p , whence $\phi(pk) = (p-1)\phi(k)$. For, if r is one of the above residues, then $r, r+k, \dots, r+(p-1)k$ form a complete set of residues modulo p and hence include a single multiple of p . Hence

$$\phi(abc\dots) = (a-1)(b-1)(c-1)\dots,$$

if a, b, c, \dots are distinct primes. Next, for $n = a^\alpha b^\beta \dots$, we use the sets of numbers from $lab\dots$ to $(l+1)ab\dots$, for $l=0, 1, \dots, a^{\alpha-1}b^{\beta-1}\dots-1$.

Borel and Drach⁸¹ noted that the period of the least residues of $0, a, 2a, \dots$ modulo N , contains N/δ terms, if δ is the g. c. d. of a, N ; conversely, if d is any divisor of N , there exist integers such that the period has d terms. Taking $a=0, 1, \dots, N-1$, we get (4).

H. Weber⁸² defined $\phi(n)$ to be the number of primitive n th roots of unity. If a is a primitive a th root of unity and β a primitive b th root, and if a, b are relatively prime, $a\beta$ is a primitive ab th root of unity and all of the latter are found in this way. Hence $\phi(ab) = \phi(a)\phi(b)$. This is also proved for relatively prime divisors a, b of $n-1$, where n is a prime, by use of integers a and β belonging to the exponents a and b respectively, modulo n , whence $a\beta$ belongs to the exponent ab .

K. Th. Vahlen⁸³ proved that, if $I_{a,\beta}(n)$ is the number of irreducible fractions between the limits α and β , $\alpha > \beta \geq 0$, with the denominator n ,

$$\sum I_{a,\beta}(d) = [(\alpha - \beta)n], \quad \sum_{k=1}^n \left[\frac{n}{k} \right] I_{a,\beta}(k) = \sum_{k=1}^n [(\alpha - \beta)k],$$

where d ranges over the divisors of n . For $\beta=0$, the first was given by Laguerre.⁸⁵ Since $I_{1,0}(n) = \phi(n)$, these formulas include (4) of Gauss and that by Dirichlet.²¹

J. J. Sylvester⁸⁴ corrected his⁸⁵ first formula to read

$$\sum_{k=1}^{\infty} T \left[\frac{j}{k} \right] = \frac{1}{2} \{ [j]^2 + [j] \} \equiv \Phi(j), \quad T[n] = \phi(1) + \dots + \phi([n]),$$

and proved it. By the usual formula for reversion,

$$T[j] = \Phi(j) - \Phi(\tfrac{1}{2}j) + \Phi(\tfrac{1}{3}j) - \Phi(\tfrac{1}{5}j) + \Phi(\tfrac{1}{6}j) - \dots$$

A. P. Minin⁸⁶ solved $\tfrac{1}{2}\phi(m) = R$ for m when R has certain values. The equation determines the number of regular star polygons of m sides.

Fr. Rogel⁸⁶ gave the formula of Dirichlet.²¹

⁸¹Introd. théorie des nombres, 1895, 23.

⁸²Lehrbuch der Algebra, I, 1895, 412, 429; ed. 2, 1898, 456, 470.

⁸³Zeitschrift Math. Phys., 40, 1895, 126-7.

⁸⁴Messenger Math., 27, 1897-8, 1-5; Coll. Math. Papers, 4, 738-742.

⁸⁵Report of Phys. Sec. Roy. Soc. of Friends of Nat. Sc., Anthropology, etc. (in Russian), Moscow, 9, 1897, 30-33. Cf. Hammond.¹²³

⁸⁶Educ. Times, 66, 1897, 62.

Rogel⁸⁷ considered the number of integers $\nu < n$ such that ν and n are not both divisible by the r th power of a prime. Also the number when each prime factor common to ν and n occurs in them exactly to the r th power.

I. T. Kaplan published at Odessa in 1897 a pamphlet in Russian on the distribution of the numbers relatively prime to a given number.

M. Bauer⁸⁸ proved that, for x prime to m , $kx+l$ represents

$$\frac{\psi(m)}{\psi(d_1 d_2)} \cdot \frac{\phi(d_1 d_2)}{\phi(m)} \cdot \phi\left(\frac{m}{d_1}\right)$$

integers relatively prime to m and incongruent modulo m , where d_1 is the g. c. d. (k, m) of k, m , and $d_2 = (l, m)$, $(d_1, d_2) = 1$, while

$$\psi(m) = \phi(m) \prod_{i=1}^s \left\{ 1 - \frac{1}{\phi(p_i)} \right\}$$

is the number of incongruent integers prime to $m = p_1^{e_1} \dots p_s^{e_s}$ which are represented by $kx+l$ when k, l, x are prime to m . Of those integers, $\psi(m)/\psi(p_1 \dots p_r)$ are divisible only by the special prime factors p_1, \dots, p_r of m .

J. de Vries^{88a} proved the first formula of Dirichlet's.²¹

C. Moreau⁸⁹ evaluated $\phi(n)$ by the method of Grunert.¹⁵

E. Landau⁹⁰ proved that

$$\sum_{n=1}^x \frac{1}{\phi(n)} = \frac{315\zeta(3)}{2\pi^4} \left(\log x + C - \sum_p \frac{\log p}{p^2 - p + 1} \right) + \epsilon,$$

where ϵ is of the order of magnitude of $x^{-1} \log x$, C is Euler's constant, and ζ is Riemann's ζ -function.

P. Wolfskehl⁹¹ proved by Tchebychef's theorem that the $\phi(n)$ integers $< n$ and prime to n are all primes only when $n = 1, 2, 3, 4, 6, 8, 12, 18, 24, 30$. [Schatunowsky.⁷⁵]

E. Landau⁹² gave a proof, without the use of Tchebychef's theorem, by finding a lower limit to the number of integers k having no square factor > 1 , where $t \leq k < 5t/8$.

E. Maillet,⁹³ by use of Tchebychef's theorem, proved the same result and the generalization: Given any integer r , there exist only a finite number of integers N such that the $\phi(N)$ integers $< N$ and relatively prime to N contain at most r equal or distinct prime factors.

Alois Pichler⁹⁴ noted that $\phi(x) = n$ has no solution if n is odd and > 1 ; while $\phi(x) = 2^n$ has the solutions $x = 2^a b c \dots (a = 0, 1, \dots, n+1)$ if

⁸⁷Sitzungsber. Böhm. Gesell., Prag, 1897; 1900, No. 30.

⁸⁸Math. Natur. Berichte aus Ungarn, 15, 1897, 41-6.

^{88a}K. Akad. Wetenschappen te Amsterdam, Verslagen, 5, 1897, 222.

⁸⁹Nouv. Ann. Math., (3), 17, 1898, 293-5.

⁹⁰Göttingen Nachrichten, 1900, 184.

⁹¹L'intermédiaire des math., 7, 1900, 253-4; Math. Ann., 54, 1901, 503-4.

⁹²Archiv Math. Phys., (3), 1, 1901, 138-142.

⁹³L'intermédiaire des math., 7, 1900, 254.

⁹⁴Ueber die Auflösung der Gl. $\phi(x) = n \dots$, Jahres-Bericht Maximilians-Gymn. in Wien, 1900-1, 3-17.

$$b=2^{2^{\beta}}+1, \quad c=2^{2^{\gamma}}+1, \dots$$

are distinct primes and $2^{\beta}+2^{\gamma}+\dots=n$ or $n-a+1$ according as $a=0$ or $a>0$. When q is a prime >3 , $\phi(x)=2q^n$ is impossible if $p=2q^n+1$ is not prime; while if p is prime it has the two solutions $p, 2p$. If $q=3$ and p is prime, it has the additional solutions $3^{n+1}, 2\cdot 3^{n+1}$. Next, $\phi(x)=2^nq$ is impossible if no one of $p_{\nu}=2^{n-\nu}q+1$ ($\nu=0, 1, \dots, n-1$) is prime and q is not a prime of the form 2^s+1 , $s=2^{\lambda}\leq n$; but if q is such a prime or if at least one p_{ν} is prime, the equation has solutions of the respective forms bq^2 , where $\phi(b)=2^{n-s}$; ap_{ν} , where $\phi(a)=2^{\nu}$. Finally, $\phi(x)=2qr$ has no solution if $p=2qr+1$ is not prime and $r\neq 2q+1$. If p is a prime, but $r\neq 2q+1$, the two solutions are $p, 2p$. If p is not prime, but $r=2q+1$, the two solutions are $r^2, 2r^2$. If p is prime and $r=2q+1$, all four solutions occur. There is a table of the values $n<200$ for which $\phi(x)=n$ has solutions.

L. Kronecker⁹⁵ considered two fractions with the denominator m as equivalent if their numerators are congruent modulo m . The number of non-equivalent reduced fractions with the denominator m is therefore $\phi(m)$. If $m=m'm''$, where m', m'' are relatively prime, each reduced fraction r/m can be expressed in a single way as a sum of two reduced partial fractions $r'/m', r''/m''$. Conversely, if the latter are reduced fractions, their sum r/m is reduced. Hence $\phi(m)=\phi(m')\phi(m'')$. The latter is also derived (pp. 245-6, added by Hensel) from (4), which is proved (pp. 243-4) by considering the g. c. d. of n with any integer $\leq n$, and also (pp. 266-7) by use of infinite series and products. Proof is given (pp. 300-1) of (5). The Gaussian median value (p. 334) of $\phi(n)/n$ is $6/\pi^2$ with an error whose order of magnitude is $1/\sqrt{n}$, provided we take as the auxiliary number of values of $\phi(n)/n$ a value of the order of magnitude $\sqrt{n} \log_e n$.

E. B. Elliott⁹⁶ considered monomials $n=p^aq^b\dots$ in the independent variables p, q, \dots . In the expansion of $n(1-1/p)^m(1-1/q)^m\dots$, the aggregate of those monomial terms whose exponents are all ≥ 0 is denoted by $F_m(n)$. Define $\mu(p^rq^s\dots)$ to be zero if any one of r, s, \dots exceeds 1, but to be $(-1)^t$ if no one of them exceeds 1, and t of them equal 1. Then

$$(7) \quad F_{m-1}(n)=\Sigma F_m(d), \quad F_{m+1}(n)=\Sigma \mu\left(\frac{n}{d}\right) F_m(d),$$

where d ranges over the monomials $p^aq^b\dots$ with $0\leq a\leq a, 0\leq b\leq b, \dots$. Henceforth, let p, q, \dots be distinct primes. Then $F_1(n)=\phi(n)$, while $F_{-1}(n)$ is the sum $\sigma(n)$ of the divisors of n . In (7), d now ranges over all the divisors of n , and $\mu(k)$ is Merten's function [Inversion]. For $m=0$, (7₂) gives the usual expression for $\phi(n)$, while (7₁) defines $\sigma(n)$. For $m=1$, (7₁) becomes (4).

If $\tau^{(1)}(n)\equiv\tau(n)$ is the number of divisors d of n , write

$$\tau^{(2)}(n)=\Sigma\tau(d), \dots, \tau^{(k)}(n)=\Sigma\tau^{(k-1)}(d).$$

⁹⁵Vorlesungen über Zahlentheorie, I, 1901, 125-6.

⁹⁶Proc. London Math. Soc., 34, 1901, 3-15.

Then

$$\tau^{(k)}(n) = \frac{\prod_a (a+k)!}{a!k!}, \quad F_{-k}(n) = \sum d \tau^{(k-1)}\left(\frac{n}{d}\right).$$

Generalizing $\mu(s)$, let $\mu^{(k)}(s)$ be zero if the expansion of the product $\prod(1-p)^k$, extended over all primes p , does not contain a term equal to s , but let it equal the coefficient of s if s occurs in the expansion. Then

$$F_k(n) = \sum d \mu^{(k)}\left(\frac{n}{d}\right).$$

The n -rowed determinant in which the element in the r th row and s th column is $F_{m-1}(\delta)$, where δ is the g. c. d. of r, s , is proved equal to $F_m(1) F_m(2) \dots F_m(n)$, a generalization of Smith's³⁹ theorem. Finally,

$$\frac{1}{n} \sum F_{k+r}\left(\frac{n}{d}\right) F_{-k}(d) = \sum \frac{1}{d} F_r(d),$$

the right member being $\tau(n)$, $\sum \phi(d)/d$, $\sum \sigma(d)/d$ for $r=0, 1, -1$.

G. Landsberg^{96a} gave a simple proof of Moreau's⁷² formula for the number of circular permutations.

L. Carlini⁹⁷ proved Dirichlet's²¹ formula by noting that

$$(8) \quad \prod_{h=1}^n (x^h - 1) = 0$$

has unity as an n -fold root, while a root $\neq 1$ of $x^h - 1$ is a root of $[n/h]$ factors $x^{th} - 1$. Hence the $\phi(h)$ primitive roots of $x^h = 1$ furnish $\phi(h)[n/h]$ roots of (8).

M. Lerch⁹⁸ found the number N of positive integers $\leq m$ which have no one of the divisors a, b, \dots, k, l , the latter being relatively prime in pairs and having m as their product. Let $F(x) = 1$ or 0 , according as x is fractional or integral. Let $L = ab \dots k$. Then [Dirichlet³³]

$$N = \frac{m(l-1)}{L} \sum_{\rho=1}^L F\left(\frac{\rho}{a}\right) \dots F\left(\frac{\rho}{k}\right) = m \left(1 - \frac{1}{a}\right) \dots \left(1 - \frac{1}{l}\right).$$

E. Landau⁹⁹ proved that the inferior limit for $x = \infty$ of

$$\frac{1}{x} \phi(x) \log_e \log_e x$$

is e^{-C} , where C is Euler's constant. Hence $\phi(x)$ is comprised between this inferior limit and the maximum $x-1$.

R. Occhipinti¹⁰⁰ proved that, if α_j is an n th root of unity, and if $d_{1i}, \dots, d_{\alpha_i}$ are the divisors of i ,

$$\prod_{j=1}^n \left\{ \sum_{i=1}^{k_1} \phi(d_{1i}) + \alpha_j \sum_{i=1}^{k_2} \phi(d_{2i}) + \dots + \alpha_j^{n-1} \sum_{i=1}^{k_n} \phi(d_{ni}) \right\} = \frac{1}{2} (-1)^{n-1} n(n+1) n^{n-2}.$$

^{96a}Archiv Math. Phys., (3), 3, 1902, 152-4.

⁹⁷Periodico di Mat., 17, 1902, 329.

⁹⁸Prag Sitzungsber., 1903, II.

⁹⁹Archiv Math. Phys., (3), 5, 1903, 86-91.

¹⁰⁰Periodico di Mat., 19, 1904, 93.

Handbuch,¹¹³ I, 217-9.

G. A. Miller¹⁰¹ proved (4) by noting that in a cyclic group G of order N there is a single cyclic subgroup of order d , a divisor of N , and it contains $\phi(d)$ operators of order d , while the order of any operator of G is a divisor of N . Thus (4) states merely that the order of G equals the sum of the numbers of the operators of the various possible orders. Next, (1) follows from an enumeration of the operators of highest period AB in a cyclic group of order AB , which is the direct product of its cyclic subgroups of orders A and B . Finally, if p is a prime, all the subgroups of a cyclic group of order p^n are contained in its subgroup of order p^{n-1} , whence $\phi(p^n) = p^n - p^{n-1}$.

G. A. Miller¹⁰² proved the last three theorems and the fact that $\phi(l)$ is even if $l > 2$ by means of the properties of the abelian group whose elements are the integers $< m$ which have with m a g. c. d. equal to k .

K. P. Nordlund¹⁰³ proved $\phi(mn \dots) = (m-1)(n-1) \dots$, where m, n, \dots are distinct primes, by writing down the multiples $< mnp$ of m , the multiples of mn , etc., whence the number of integers $< mnp$ and not prime to it is $mnp - 1 - (m-1)(n-1)(p-1)$.

E. Busche¹⁰⁴ treated geometrically systems $\left(\begin{smallmatrix} ac \\ bd \end{smallmatrix}\right)$ of four integers such that $ad - bc > 0$, evaluated the number $\Phi(S)$ of systems incongruent modulo S and prime to S , and generalized (4) to $\Sigma \Phi(S)$.

L. Orlando¹⁰⁵ showed that $\phi(m)$ is determined by (4) [Lucas⁷²].

H. Bonse¹⁰⁶ proved Maillet's⁹³ theorem for $r=1, 2, 3$ without using Tchebychef's theorem. His lemma was generalized by T. Suzuki.^{106a}

J. Sommer¹⁰⁷ gave without reference Crelle's⁸ final evaluation of $\phi(n)$.

R. D. Carmichael¹⁰⁸ proved that if n is such that $\phi(x) = n$ is solvable there are at least two solutions x . He found solutions of $\phi(x) = 2^n$ [in accord with Pichler⁹⁴] and proved that there are just $n+2$ solutions (a single one being odd) when $n \leq 31$ and just 33 solutions when $32 \leq n \leq 255$. All the solutions of $\phi(x) = 4n - 2 > 2$ are of the form $p^a, 2p^a$, where p is a prime of the form $4s-1$; for example, if $n=5$, the solutions are 19, 27 and their doubles.

Carmichael¹⁰⁹ gave a table showing every value of m for which $\phi(m)$ has any given value ≤ 1000 .

A. Ranum^{109a} would solve $\phi(x) = n$ by resolving n in every possible way into factors n_0, \dots, n_r , capable of being taken as the values of $\phi(2^{a_0}), \phi(p_1^{a_1}), \dots, \phi(p_r^{a_r})$, where $2, p_1, \dots, p_r$ are distinct primes. Then $2^{a_0} p_1^{a_1} \dots p_r^{a_r}$ is a value of x .

Carmichael¹¹⁰ gave a method of solving $\phi(x) = a$, based on the testing of the equation for each factor x of a definite function of a .

M. Fekete¹¹¹ considered the determinant ρ_{kn} obtained by deleting the last row and last column of Sylvester's eliminant for $x^k - 1 = 0$ and $x^n - 1 = 0$

¹⁰¹Amer. Math. Monthly, 12, 1905, 41-43.

¹⁰²Amer. Jour. Math., 27, 1905, 315.

¹⁰³Nyt Tidskrift for Mat., 16A, 1905, 15-29.

¹⁰⁴Jour. für Math., 131, 1906, 113-135.

¹⁰⁵Periodico di Mat., 22, 1907, 134-6.

¹⁰⁶Archiv Math. Phys., (3), 12, 1907, 292-5.

^{106a}Tôhoku Math. Jour., 3, 1913, 83-6.

¹⁰⁷Vorlesungen über Zahlentheorie, 1907, 5.

¹⁰⁸Bull. Amer. Math. Soc., 13, 1907, 241-3.

¹⁰⁹Amer. Jour. Math., 30, 1908, 394-400.

^{109a}Trans. Amer. Math. Soc., 9, 1908, 193-4.

¹¹⁰Bull. Amer. Math. Soc., 15, 1909, 223.

¹¹¹Math. és Phys. Lapok (Math. Phys. Soc.), Budapest, 18, 1909, 349-370. German transl., Math. Naturwiss. Berichte aus Ungarn, 26, 1913 (1908), 196.

($k < n$). Thus $|\rho_{kn}| = 1$ or 0 according as k and n are relatively prime or not. Hence

$$\phi(n) = \sum_{k=1}^n |\rho_{kn}|, \quad \phi_1(n) = \sum_{k=1}^n k |\rho_{kn}|,$$

where $\phi_1(n)$ is the sum of the integers $\leq n$ and prime to n .

R. Remak¹¹² proved Maillet's⁹³ theorem without using Tchebychef's.

E. Landau¹¹³ proved (5), Wolfskehl's⁹¹ theorem and Maillet's⁹³ generalization.

C. Orlandi¹¹⁴ proved that, if x ranges over all the positive integers for which $[m/x]$ is odd, then $\Sigma \phi(x) = (m/2)^2$ for m even (Cesàro, p. 144 of this History), while $\Sigma \phi(x) = k^2$ for $m = 2k - 1$.

A. Axer¹¹⁵ considered the system (P) of all integers relatively prime to the product P of a finite number of given primes and obtained formulas and asymptotic theorems concerning the number of integers $\leq x$ of (P) which are prime to x . Application is made to the probability that two numbers $\leq n$ of (P) are relatively prime and to the asymptotic values of the number (i) of positive irreducible fractions with numerator and denominator in (P) and $\leq n$ and (ii) of regular continued fractions representing positive fractions in (P) with numerator and denominator $\leq n$.

G. A. Miller¹¹⁶ defined the order of a modulo m to be the least positive integer b such that $ab \equiv 0 \pmod{m}$. If p^a is the highest power of a prime p dividing m , the numbers $\leq m$ whose orders are powers of p are km/p^a ($k = 1, 2, \dots, p^a$). Hence $\Sigma k_i m/p_i^{a_i}$ ($k_i = 1, \dots, p_i^{a_i}$) form a complete set of residues modulo $m = \Pi p_i^{a_i}$. If the orders of two integers are relatively prime, the order of their sum is congruent modulo m to the product of their orders. But the number of integers $\leq m$ whose orders equal m is $\phi(m)$. Hence $\phi(\Pi p^a) = \Pi \phi(p^a)$. Since all numbers $\leq m$ whose orders divide d , a divisor of m , are multiples of m/d , there are exactly d numbers $\leq m$ whose orders divide d , and $\phi(d)$ of them are of order d . Hence $m = \Sigma \phi(d)$.

S. Composto¹¹⁷ employed distinct primes m, n, r , and the $\nu = \phi(mn)$ integers p_1, \dots, p_ν prime to mn and $\leq mn$, and proved that

$$p_i, p_i + mn, p_i + 2mn, \dots, p_i + (r-1)mn \quad (i = 1, \dots, \nu)$$

include all and only the numbers rp_1, \dots, rp_ν and the numbers not exceeding and prime to mnr . Hence $\phi(mnr) = \phi(mn) \cdot (r-1)$. A like theorem is proved for two primes and stated for any number of primes. [The proof is essentially Euler's¹ proof of (1) for the case in which B is a prime not dividing a product A of distinct primes.] Next, if d is a prime factor of n , the integers not exceeding and prime to dn are the numbers $\leq n$ and prime to n , together with the integers obtained by adding to each of them $n, 2n, \dots$,

¹¹²Archiv Math. Phys., (3), 15, 1909, 186-193.

¹¹³Handbuch. . . Verteilung der Primzahlen, I, 1909, 67-9, 229-234.

¹¹⁴Periodico di Mat., 24, 1909, 176-8.

¹¹⁵Monatshefte Math. Phys., 22, 1911, 3-25.

¹¹⁶Amer. Math. Monthly, 18, 1911, 204-9.

¹¹⁷Il Boll. di Matematica Gior. Sc.-Didat., 11, 1912, 12-33.

$(d-1)n$; whence $\phi(dn) = d\phi(n)$. Finally, let p_1, \dots, p_r be the $\nu = \phi(n)$ integers $< n$ and prime to n . Then $p_i + kn$ ($i = 1, \dots, \nu$; $k = 0, 1, \dots$) give all integers prime to n ; let $P_h(n)$ denote the h th one of them arranged in order of magnitude. Then

$$P_{k\nu}(n) = kn - 1 \quad (k \geq 1), \quad P_{k\nu+r}(n) = kn + p_r \quad (1 \leq r \leq \nu - 1, k \geq 0).$$

If $h = k\nu + r$, $r < \nu$, the sum of the first h numbers prime to n is

$$kn \left\{ \frac{k\nu}{2} + r \right\} + p_1 + \dots + p_r,$$

where p_1, \dots, p_r are the first r integers $< n$ and prime to n .

K. Hensel¹¹⁸ evaluated $\phi(n)$ by the first remark of Crelle.¹⁷

J. G. van der Corput and J. C. Kuyver¹¹⁹ proved that the number $I(a/4)$ of integers $\leq a/4$ and prime to a is $N = \frac{1}{4}a\Pi(1 - 1/p)$ if a has a prime factor $4m+1$, where p ranges over the distinct prime factors of a ; but is $N - 2^{k-2}$ if a is a product of powers of k prime factors all of the form $4m-1$. Also $I(a/6)$ is evaluated.

U. Scarpis¹²⁰ noted that $\phi(p^n - 1)$ is divisible by n if p is a prime.

Several writers¹²¹ discussed the solution of $\phi(x) = \phi(y)$, where x, y are powers of primes. Several¹²² proved that $\phi(xy) > \phi(x)\phi(y)$ if x, y have a common factor.

J. Hammond¹²³ proved that there are $\frac{1}{2}\phi(n) - 1$ regular star n -gons.

H. Hancock¹²⁴ denoted by $\Phi(i, k)$ the number of triples $(i, k, 1), (i, k, 2), \dots, (i, k, i)$ whose g. c. d. is unity. Let $i = i_1d, k = k_1d$, where i_1, k_1 are relatively prime. Then $\Phi(i, k) = i_1\phi(d), \Phi(k, i) = k_1\phi(d)$.

A. Fleck¹²⁵ considered the function, of $m = \Pi p^a$,

$$\phi_k(m) = \prod_p \left\{ \phi(p^a) - \binom{k}{1} \phi(p^{a-1}) + \dots + (-1)^a \binom{k}{a} \phi(p^{a-a}) \right\}.$$

Thus $\phi_0(m) = \phi(m), \phi_{-1}(m) = m, \phi_{-2}(m)$ is the sum of the divisors of m . Also

$$\sum_{d|m} \phi_k(d) = \phi_{k-1}(m), \quad \phi_k(mn) = \phi_k(m)\phi_k(n),$$

if m, n are relatively prime. For $\zeta(s) = \sum m^{-s}$,

$$\sum_{m=1}^{\infty} \frac{\phi_{k-1}(m)}{m^s} = \zeta(s) \sum_{m=1}^{\infty} \frac{\phi_k(m)}{m^s},$$

$$\phi_k(p) = p - \binom{k+1}{1}, \quad \phi_k(p^2) = p^2 - \binom{k+1}{1}p + \binom{k+1}{2}, \quad \dots,$$

$$\phi_k(p^{k+1+\mu}) = p^\mu(p-1)^{k+1}.$$

¹¹⁸Zahlentheorie, 1913, 97.

¹¹⁹Wiskundige Opgaven, 11, 1912-14, 483-8.

¹²⁰Periodico di Mat., 29, 1913, 138.

¹²¹Amer. Math. Monthly, 20, 1913, 227-8 (incomplete); 309-10.

¹²²Math. Quest. Educat. Times, 24, 1913, 72, 106.

¹²³Ibid., 25, 1914, 69-70.

¹²⁴Comptes Rendus Paris, 158, 1914, 469-470.

¹²⁵Sitzungsber. Berlin Math. Gesell., 13, 1914, 161-9.

E. Cahen¹²⁶ gave F. Arndt's¹⁹ proof without reference.

A. Cunningham¹²⁷ tabulated all solutions N of $\phi(N) = 2^r$ for $r = 4, 6, 8, 9, 10, 11, 12, 16$, each solution being a product of a power of 2 by distinct primes $2^{2^n} + 1$.

J. Hammond¹²⁸ noted that, if $\Sigma f(k/n) = F(n)$ or $\Phi(n)$, according as the summation extends over all positive integers k from 1 to n or only over such of them as are prime to n , then $\Sigma \Phi(d) = F(n)$. This becomes (4) when f is constant.

R. Ratat¹²⁹ noted that $\phi(n) = \phi(n+1)$ for $n = 1, 3, 15, 104$. For $n < 125$, $2n \neq 2, 4, 16, 104$, he verified that $\phi(2n \pm 1) > \phi(2n)$.

R. Goormaghtigh¹³⁰ noted that $\phi(n) = \phi(n+1)$ also for $n = 164, 194, 255$ and 495. He gave very special results on the solution of $\phi(x) = 2a$.

Formulas involving ϕ are cited under Lipschitz,^{50, 56} Cesàro,⁶¹ Hammond,¹¹¹ and Knopp¹⁶⁰ of Ch. X, Hammond⁴³ of Ch. XI, and Rogel¹²⁴³ of Ch. XVIII. Cunningham⁹⁵ of Ch. VII gave the factors of $\phi(p^k)$. Dedekind⁷¹ of Ch. VIII generalized ϕ to a double modulus. Minin¹²⁰ of Ch. X solved $\phi(N) = \tau(N)$.

SUM $\phi_k(n)$ OF THE k TH POWERS OF THE INTEGERS $\leq n$ AND PRIME TO n .

A. Cauchy¹⁴⁹ noted that $\phi_1(n)$ is divisible by n if $n > 2$, since the integers $< n$ and prime to n may be paired so that the sum of the two of any pair is n .

A. L. Crelle¹⁷ (p. 80, p. 84) noted that $\phi_1(n) = \frac{1}{2}n\phi(n)$. The proof follows from the remark by Cauchy.

A. Thacker¹⁵⁰ defined $\phi_k(n)$ and noted that it reduces for $k=0$ to Euler's $\phi(n)$. Set $s_k(z) = 1^k + 2^k + \dots + z^k$, $n = a^\alpha b^\beta c^\gamma \dots$, where a, b, \dots are distinct primes. By deleting the multiples of a , then the remaining multiples of b , etc., he proved that

$$\phi_k(n) = s_k(n) - \sum_a a^k s_k\left(\frac{n}{a}\right) + \sum_{a,b} a^k b^k s_k\left(\frac{n}{ab}\right) - \sum_{a,b,c} a^k b^k c^k s_k\left(\frac{n}{abc}\right) + \dots,$$

where the summation indices range over the combinations of a, b, c, \dots one, two, ... at a time. In the second paper, he proved Bernoulli's^{150a} formula

$$s_k(z) = \frac{z^{k+1}}{k+1} + \frac{1}{2}z^k + \frac{1}{2}\binom{k}{1}B_1z^{k-1} - \frac{1}{4}\binom{k}{3}B_3z^{k-3} + \frac{1}{6}\binom{k}{5}B_5z^{k-5} - \dots,$$

where B_1, B_3, \dots are the Bernoullian numbers. Then, by substitution,

$$\phi_k(n) = \frac{n^{k+1}}{k+1} \Pi\left(1 - \frac{1}{a}\right) + \frac{1}{2}\binom{k}{1}B_1n^{k-1}\Pi(1-a) - \frac{1}{4}\binom{k}{3}B_3n^{k-3}\Pi(1-a^3)$$

¹²⁶Théorie des nombres, I, 1914, 393.

¹²⁷Math. Quest. Educ. Times, 27, 1915, 103-6.

¹²⁸Ibid., 29, 1916, 53.

¹²⁹L'intermédiaire des math., 24, 1917, 101-2.

¹³⁰Ibid., 25, 1918, 42-4.

¹⁴⁹Mém. Ac. Sc. de l'Institut de France, 17, 1840, 565; Oeuvres, (1), 3, 272.

¹⁵⁰Jour. für Math., 40, 1850, 89-92; Cambridge and Dublin Math. Jour., 5, 1850, 243. Reproduced, with errors as to signs, by Zerr, Amer. Math. Monthly, 5, 1898, 93-5. Cf. E. Prouhet, Nouv. Ann. Math., 10, 1851, 324-330.

^{150a}Jacques Bernoulli, Ars conjectandi, 1713, 95-7.

$$+\frac{1}{6}\binom{k}{5}B_5n^{k-5}\Pi(1-a^5)-\dots,$$

where $\Pi(1-a^i)$ denotes $(1-a^i)(1-b^i)\dots$.

J. Binet¹⁵¹ wrote η_1, \dots, η_n for the integers $< N$ and prime to $N = p^\lambda q^\mu \dots$. Then, if $B_1, -B_3, B_5, \dots$ are the Bernoullian numbers $1/6, 1/30, 1/42, \dots$, and $P_g = (1-p^g)(1-q^g)\dots$,

$$\sum_{i=1}^n \frac{1}{(x+\eta_i)^2} = \left(\frac{1}{x} - \frac{1}{x+N}\right)P_{-1} + \left(\frac{1}{x^3} - \frac{1}{(x+N)^3}\right)B_1P_1 \\ + \left(\frac{1}{x^5} - \frac{1}{(x+N)^5}\right)B_3P_3 + \dots,$$

for x sufficiently small to insure convergence. Expanding each member into negative powers of x and comparing coefficients, we get

$$n = \sum \eta_i^0 = P_{-1}N, \quad 2\sum \eta_i^2 = P_{-1}N^2, \quad 3\sum \eta_i^3 = P_{-1}N^3 + 3B_1P_1N, \\ 4\sum \eta_i^3 = P_{-1}N^4 + 6B_1P_1N^2, \dots$$

the first being equivalent to the usual formula for $\phi(N)$. The general law can be represented symbolically by

$$g \sum_{i=1}^n \eta_i^{g-1} = \frac{1}{2BP} \{ (N+BP)^g + (N-BP)^g \},$$

where, after expanding the binomials, we are to replace $N^g/(BP)$ by $P_{-1}N^g$ and any other term $(BP)^{2h-1}$ by $B_{2h-1}P_{2h-1}$. It is easily shown that, if k is odd, $\sum \eta_i^k$ is divisible by N .

Silva²⁵ used his symbolic formula, taking S to be the sum of $1, \dots, n$, whence $S(a)$ is the sum $\frac{1}{2}n(1+n/A)$ of the multiples $\leq n$ of A . Thus $\phi_1(n) = \frac{1}{2}n\phi(n)$. This proof of Crelle's result is thus like that by Brennecke.¹⁵²

W. Brennecke¹⁵² proved Crelle's result by means of

$$1 + \dots + n - \{a\left(1+2+\dots+\frac{n}{a}\right) + b\left(1+\dots+\frac{n}{b}\right) + \dots\} \\ + \{ab\left(1+\dots+\frac{n}{ab}\right) + \dots\} + \dots$$

Set $\mu = \phi(n)$, $a = abc \dots$. He proved that

$$\phi_2(n) = \frac{1}{3}\mu(n^2 \pm a/2), \quad \phi_3(n) = \frac{1}{4}\mu n(n^2 \pm a),$$

$$\phi_4(n) = \frac{1}{5}\mu n^4 \pm \frac{1}{3}a\mu n^2 - \frac{1}{30}n(1-a^3)(1-b^3)\dots,$$

the signs being $+$ or $-$ according as the number of the distinct prime factors a, b, \dots of n is even or odd.

¹⁵¹Comptes Rendus Paris, 32, 1851, 918-921.

¹⁵²Programm Realschule, Posen, 1855, §§5-6.

G. Oltramare¹⁵³ obtained for the sum, sum of squares, sum of cubes, and sum of biquadrates, of the integers $< ma$ and relatively prime to a the respective values

$$\begin{aligned}\frac{1}{2}m^2a\phi(a), & \quad \frac{1}{3}m^3a^2\phi(a) + (-1)^a \frac{m}{2 \cdot 3}a\phi(a_1), \\ \frac{1}{4}m^4a^3\phi(a) + (-1)^a \frac{m^2}{4}a^2\phi(a_1), \\ \frac{1}{5}m^5a^4\phi(a) + (-1)^a \frac{m^3}{3}a^3\phi(a_1) - (-1)^a \frac{m}{2 \cdot 3 \cdot 5}a\xi(a_1),\end{aligned}$$

where a is the number and a_1 the product of the distinct prime factors μ, ν, \dots of a , while $\xi(a_1) = (\mu^3 - 1)(\nu^3 - 1) \dots$. The number of integers $< n$ which are prime to a is $\phi(a)n/a$.

J. Liouville¹⁵⁴ stated that Gauss' proof of $\sum \phi(d) = N$ may be extended to the generalization

$$\sum \left(\frac{N}{d} \right)^k \phi_k(d) = 1^k + 2^k + \dots + N^k,$$

where d ranges over the divisors of N . He remarked that Binet's¹⁵¹ results are readily proved in various ways. Also,

$$\sum \left(\frac{m}{d} \right)^3 \phi_3(d) = \left\{ \sum \frac{m}{d} \phi(d) \right\}^2.$$

N. V. Bougaief¹⁵⁵ stated that, if $\xi(n)$ is the number of distinct prime factors of $n > 1$, and $\xi_1(n)$ is their product,

$$6\phi_2(n) = 2\phi(n)n^2 + (-1)^{\xi(n)}\xi_1(n)\phi(n);$$

also a result quoted below with Gegenbauer's¹⁷⁰ generalization.

August Blind¹⁵⁶ reproduced without reference the formulas and proofs by Thacker,¹⁵⁰ and gave

$$\phi_r(m) = m^r \phi_0(m) - \binom{r}{1} m^{r-1} \phi_1(m) + \binom{r}{2} m^{r-2} \phi_2(m) - \dots + (-1)^r \phi_r(m).$$

E. Lucas¹⁵⁷ indicated a proof that $n\phi_{n-1}(x)$ is given symbolically by $(x+Q)^n - Q^n$, where, if $n = a^\alpha b^\beta \dots$, $Q_k = B_k(1 - a^{k-1})(1 - b^{k-1}) \dots$. Thus, if π is the product of the negatives of the primes a, b, \dots ,

$$2\phi_1(x) = x\phi(x), \quad 3\phi_2(x) = \phi(x) \left(x^2 + \frac{1}{2}\pi \right), \quad 4\phi_3(x) = x\phi(x)(x^2 + \pi).$$

¹⁵³Mémoires de l'Institut Nat. Génevois, 4, 1856, 1-10.

¹⁵⁴Comptes Rendus Paris, 44, 1857, 753-4; Jour. de Math., (2), 2, 1857, 393-6.

¹⁵⁵Nouv. Ann. Math., (2), 13, 1874, 381-3; Bull. Sc. Math. Astr., 10, I, 1876, 18.

¹⁵⁶Ueber die Potenzsummen der unter einer Zahl m liegenden und zu ihr relativ primen Zahlen, Diss., Bonn, 1876, 37 pp.

¹⁵⁷Nouv. Ann. Math., (2), 16, 1877, 159; Théorie des nombres, 1891, 394.

Several^{157a} found expressions for $\phi_n = \phi_n(N)$ and proved that

$$\phi_0 x^n + n\phi_1 x^{n-1} + \frac{1}{2}n(n-1)\phi_2 x^{n-2} + \dots + \phi_n = 0 \quad (n \text{ odd})$$

has the root $-\phi_1/\phi_0$, while the remaining roots can be paired so that the sum of the two of any pair is $-2\phi_1/\phi_0$. If $n=3$ the roots are in arithmetical progression.

H. Postula¹⁵⁸ proved Crelle's result by the long method of deleting multiples, used by Brennecke.¹⁵² Catalan (*ibid.*, pp. 208-9) gave Crelle's short proof.

Mennesson¹⁵⁹ stated that, if q is any odd number,

$$\phi_q(n) \equiv \frac{1}{2}\phi(n^{q+1}) \pmod{q},$$

and (Ex. 366) that the sum of the products $\phi(n) - 1$ at a time of the integers $\leq n$ and prime to n is a multiple of n .

E. Cesàro¹⁶⁰ proved the generalization: The sum ψ_m of the products m at a time of the integers $\alpha, \beta, \dots \leq N$ and prime to N is divisible by N if m is odd. For by replacing α by $N-\alpha$, β by $N-\beta$, \dots and expanding,

$$\psi_m = \binom{\phi}{m} N^m - \binom{\phi-1}{m-1} N^{m-1} \psi_1 + \binom{\phi-2}{m-2} N^{m-2} \psi_2 - \dots \pm \psi_m,$$

where $\phi = \phi(N)$. Also $\phi_m(N)$ is divisible by N if m is odd.

F. de Rocquigny¹⁶¹ proved Crelle's result. Later, he¹⁶² employed concentric circles of radii 1, 2, 3, \dots and marked the numbers $(m-1)N+1$, $(m-1)N+2$, \dots , mN at points dividing the circle of radius m into N equal parts. The lines joining the center to the $\phi(N)$ points on the unit circle, marked by the numbers $< N$ and prime to N , meet the various circles in points marked by all the numbers prime to N . He stated that the sum of the $\phi(N)$ numbers prime to N appearing on the circle of radius m is $\frac{1}{2}(2m-1)\phi(N^2)$, and [the equivalent result] that the sum of the numbers prime to N from 0 to mN is $\frac{1}{2}m^2\phi(N^2)$. He later recurred to the subject (**ibid.*, 54, 1881, 160).

A. Minine¹⁶³ noted that, if $P > N > 1$ and k is the remainder obtained by dividing P by N , the sum $s(N, P)$ of the integers $< P$ and prime to N may be computed by use of

$$s(N, mN+k) = s(N, k) + \frac{m^2}{2}\phi(N^2) + mN\phi(N)_k,$$

where (Minine⁴⁷) $\phi(N)_k$ is the number of integers $\leq k$ prime to N .

*A. Minine¹⁶⁴ considered the number and sum of all the integers $< P$ which are prime to N [Legendre's (5) and Minine¹⁶³].

^{157a}Math. Quest. Educ. Times, 28, 1878, 45-7, 103-5.

¹⁵⁸Nouv. Corresp. Math., 4, 1878, 204-7. Likewise, R. A. Harris, Math. Mag., 2, 1904, 272.

¹⁵⁹*Ibid.*, p. 302.

¹⁶⁰*Ibid.*, 5, 1879, 56-59.

¹⁶¹Les Mondes, Revue Hebdom. des Sciences, 51, 1880, 335-6.

¹⁶²*Ibid.*, 52, 1880, 516-9.

¹⁶³*Ibid.*, 53, 1880, 526-9.

¹⁶⁴Nouveaux théorèmes de la théorie des nombres, Moscow, 1881.

A. Minine¹⁶⁵ investigated the numbers N which divide the sum of all the integers $< N$ and prime to N .

E. Cesàro¹⁶⁶ proposed his theorems¹⁶⁰ as exercises. Proofs, by associating α with $N-\alpha$, etc., were given by Moret-Blanc (3, 1884, 483-4).

Cesàro⁵⁷ (p. 82) proved the formula of Liouville.¹⁵⁴ Writing (pp. 158-9) ϕ_m for $\phi_m(N)$ and expanding $\phi_m = \Sigma(N-\alpha)^m$, where α, β, \dots are the integers $\leq N$ and prime to N , we get

$$\phi_m = N^m \phi - \binom{m}{1} N^{m-1} \phi_1 + \binom{m}{2} N^{m-2} \phi_2 - \dots \pm \phi_m,$$

whence ϕ_m is divisible by N if m is odd, but not if m is even. This is evident (p. 257) since $\alpha^m + (N-\alpha)^m$ is divisible by $\alpha + N - \alpha$ if m is odd. The above formula gives $A^m = (1-A)^m$, symbolically, where

$$A_m = \frac{\phi_m}{\phi} \cdot \frac{1}{N^m}$$

is the arithmetic mean of the m th powers of $\alpha/N, \beta/N, \dots$. The mean value of $\phi_m(N)$ is $6A_m N^{m+1}/\pi^2$. He reproduced (pp. 161-2) an earlier formula,¹⁶⁰ which shows that $B^m = (1-B)^m$, symbolically, if B_m is the arithmetic mean of the products of $\alpha/N, \beta/N, \dots$ taken m at a time. We have (p. 165) the approximation

$$\sum_{j=1}^z \phi_m(j) = \frac{x^{m+2}}{(m+1)(m+2)} \cdot \frac{6}{\pi^2},$$

whence (p. 261) the mean of $\phi_m(N)$ is $6N^{m+2}/(m+1)\pi^2$.

Proof is given (pp. 255-6) of Thacker's¹⁵⁰ formula

$$\phi_m(N) = \frac{(N+B\psi)^{m+1} - (B\psi)^{m+1}}{m+1} = \frac{1}{m+1} \sum_{p=0}^m \binom{m+1}{p} B_p N^{m-p+1} \psi_p(N),$$

where

$$\psi_p(N) = \Sigma d^{p-1} \mu(d) = \Pi(1-u^{p-1}),$$

d ranging over the divisors of N , and u over the prime divisors of N . Here $\mu(x)$ is Merten's function (Ch. XIX). It is proved (pp. 258-9) that

$$\Sigma d^{p-1} \psi_p\left(\frac{N}{d}\right) = 1, \quad \Sigma d^k \psi_s\left(\frac{N}{d}\right) = \Sigma d^k \psi_{s-k}(d),$$

the first characterizing the function $\psi_p(N)$, and reducing to (4) for $p=0$. If α ranges over the integers for which $[2n/\alpha]$ is odd, then (p. 293)

$$\Sigma \phi_m(\alpha)/\alpha^m = \frac{n^2}{m+1} - \frac{m}{12} \Delta_n,$$

exactly if $m=0, 1, 2, 3$, approximately if $m>3$, where Δ_n is the excess of the sum of the inverses of $1, \dots, n$ over that of $n+1, \dots, 2n$. In particular, $\Sigma \phi(\alpha) = n^2$.

¹⁶⁵Math. Soc. Moscow (in Russian), 10, 1882-3, 87-101.

¹⁶⁶Nouv. Ann. Math., (3), 2, 1883, 288.

P. Nazimov¹⁶⁷ (Nasimof) noted that, when x ranges over the integers $\leq m$ and prime to n , the sum of the values taken by any function $f(x)$ equals

$$\sum_d \mu(d) \sum_{x=1}^{[m/d]} f(dx),$$

where d ranges over all divisors of n . The case $f(x) \equiv 1$ yields Legendre's formula (5). The case $f(x) \equiv x$ yields a result equivalent to that of Minine.¹⁶³⁻⁴ A generalization was given by Zsigmondy⁷⁷ and Gegenbauer.¹⁷³

E. Cesàro¹⁶⁸ noted that, if A_m is the arithmetic mean of the m th powers of the integers $\leq N$ and prime to N , and B_m that of their products m at a time, we have the symbolic relations

$$A^m = (N - A)^m, \quad B^m = (N - B)^m.$$

Cesàro¹⁶⁹ proved Thacker's¹⁵⁰ formula expressed as

$$\phi_k(n) = \frac{n^k}{n+1} \sum_{i=0}^k \binom{k+1}{i} B_i \zeta_i(n) = \frac{n^k}{k+1} \{ (1+B\zeta)^{k+1} - (B\zeta)^{k+1} \},$$

the last being symbolic, where ζ_k is a function such that $\sum \zeta_k(d) = n^{1-k}$, d ranging over the divisors of n . By inversion

$$\zeta_k(n) = \sum_d \mu\left(\frac{n}{d}\right) d^{1-k} = \frac{1}{n^{k-1}} \Pi (1 - u^{k-1}),$$

where u ranges over the distinct prime factors of n .

L. Gegenbauer¹⁷⁰ proved that, if $\nu = \left[\sqrt[p]{n} \right]$,

$$\sum_{x=1}^n \{ 1^k + 2^k + \dots + (g_\rho(x))^k \} = \sum_{n=1}^{\nu} \left[\frac{n}{x^\rho} \right] \phi_k(x), \quad g_\rho(p_1^{a_1} \dots p_s^{a_s}) \equiv \prod_{i=1}^s p_i^{\left[\frac{a_i}{\rho} \right]}.$$

For the case $k=0$, $\rho=2$, this becomes Bougaief's¹⁵⁵ formula

$$\sum_{x=1}^n g_2(x) = \sum_{x=1}^{\nu} \left[\frac{n}{x^2} \right] \phi(x), \quad \nu = [\sqrt{n}].$$

C. Leudesdorf¹⁷¹ considered for μ odd the sum $\psi_\mu(N)$ of the inverses of the μ th powers of the integers $< N$ and prime to N . Then

$$\psi_\mu(N) = \frac{1}{2} k N^2 - \frac{1}{2} \mu N \psi_{\mu+1}(N),$$

where k is an integer. Thus, if $N = p^l q$, where q is not divisible by the prime $p > 3$, $\psi_\mu(N)$ is divisible by p^{2l} unless μ is prime to p , and $\mu+1$ is divisible by $p-1$; for example, $\psi_\mu(p)$ is divisible by p^2 . If $p=3$, $\psi_\mu(N)$ is divisible by p^{2l} if μ is an odd multiple of 3. If $p=2$, it is divisible by 2^{2l-1} except when $q=1$.

Cesàro¹⁷² inverted his⁵⁷ symbolic form of Thacker's formula for $\phi_m(N)$ in terms of ψ 's and obtained

$$n B_p \psi_p(n) = (\phi - n B)^p.$$

¹⁶⁷Matem. Sbornik (Math. Soc. Moscow), 11, 1883-4, 603-10 (Russian).

¹⁶⁸Mathesis, 5, 1885, 81.

¹⁶⁹Giornale di Mat., 23, 1885, 172-4.

¹⁷⁰Sitzungsber. Ak. Wiss. Wien (Math.), 95, II, 1887, 219-224.

¹⁷¹Proc. London Math. Soc., 20, 1889, 199-212.

¹⁷²Periodico di Mat., 7, 1892, 3-6. See p. 144 of this history.

Hence if a ranges over the integers $\leq n$ and prime to n ,

$$\Sigma(a - nB)^p = 0 \text{ or a multiple of } n\psi_p$$

according as p is odd or even. By this recursion formula,

$$\phi_1 = \frac{1}{2}n\phi, \quad \phi_3 = \frac{3}{2}n\phi_2 - \frac{1}{4}n^3\phi, \dots$$

L. Gegenbauer¹⁷³ gave a formula including those of Nazimov¹⁶⁷ and Zsigmondy.⁷⁷ For any functions $\chi(d)$, $\chi_1(d)$, $f(x_1, \dots, x_s)$,

$$\sum_{x_1, \dots, x_s}^{1, \dots, m} f(\kappa x_1, \dots, \kappa x_s) \sum_{\delta} \chi(\delta) \chi_1\left(\frac{n}{\delta}\right) = \sum_d \chi(d) \chi_1\left(\frac{n}{d}\right) \sum_{x_1, \dots, x_s}^{1, \dots, [m/d]} f(d\kappa x_1, \dots, d\kappa x_s),$$

where d ranges over all divisors of n which have some definite property P , while δ ranges over those common divisors of n , x_1, \dots, x_s which have property P . Various special choices are made for χ , χ_1 , f and P . For instance, property P may be that d is an exact ρ th power, whence, if $\rho = 1$, d is any divisor of n . The special results obtained relate mainly to new number-theoretic functions without great interest and suggested apparently by the topic in hand.

T. del Beccaro¹⁷⁴ noted that $\phi_k(n)$ is divisible by n if k is odd [Binet¹⁵¹]. When n is a power of 2,

$$1^k + 2^k + \dots + (n-1)^k \equiv 0 \text{ or } \phi(n) \pmod{n},$$

according as k is odd or even. His proof of (1) is due to Euler.

J. W. L. Glaisher¹⁷⁵ proved that, if a, b, \dots are any divisors of x such that their product is also a divisor, the sum of the n th powers of the integers $< x$ and not divisible by a or b, \dots , is

$$\frac{1}{n+1} \left[x^{n+1} \Pi \left(1 - \frac{1}{a} \right) + (-1)^s \left\{ \binom{n+1}{2} F_1 x^{n-1} - \binom{n+1}{4} F_2 x^{n-3} - \dots \right\} \right],$$

where s is the number of the divisors a, b, \dots , and

$$F_n = B_n(a^{2n-1} - 1)(b^{2n-1} - 1) \dots$$

If a, b, \dots are all the prime factors of x , this result becomes Thacker's.¹⁵⁰

N. Nielsen¹⁷⁶ proved by induction on γ that the sum of the n th powers of the positive integers $< mM$ and prime to $M = p_1^{t_1} \dots p_r^{t_r}$ is

$$\frac{m^{n+1} M^n \phi(M)}{n+1} + (-1)^\gamma \sum_{s=1}^{[n/2]} \frac{(-1)^{s-1}}{n+1} \binom{n+1}{2s} B_s (mM)^{n-2s+1} \prod_{i=1}^{\gamma} (p_i^{2s-1} - 1).$$

The case $m = 1$ gives Thacker's¹⁵⁰ result. That result shows (*ibid.*, p. 179) that $\phi_{2n}(m)$ and $\phi_{2n+1}(m)$ are divisible by m and m^2 respectively, for $1 \leq n \leq (p_1 - 3)/2$, where p_1 is the least prime factor of m , and also gives the residues of the quotients modulo m . Corresponding theorems therefore hold for the sum of the products of the integers $< m$ and prime to m , taken t at a time.

¹⁷³Sitzungsberichte Ak. Wiss. Wien (Math.), 102, 1893, IIa, 1265-94.

¹⁷⁴Atti R. Accad. Lincei, Mem. Cl. Fis. Mat., 1, 1894, 344-371.

¹⁷⁵Messenger Math., 28, 1898-9, 39-41.

¹⁷⁶Oversigt Danske Vidensk. Selsk. Föreläsningar, 1915, 509-12; cf. 178-9.

SCHEMMEL'S GENERALIZATION OF EULER'S ϕ -FUNCTION.

V. Schemmel¹⁹⁰ considered the $\Phi_n(m)$ sets of n consecutive numbers each $< m$ and relatively prime to m . If $m = a^\alpha b^\beta \dots$, where a, b, \dots are distinct primes, and m, m' are relatively prime, he stated that

$$\begin{aligned} \Phi_n(m) &= a^{\alpha-1}(a-n)b^{\beta-1}(b-n) \dots, & \Phi_n(mm') &= \Phi_n(m)\Phi_n(m'), \\ \sum_{\delta} n^{\alpha-\alpha'} n^{\beta-\beta'} \dots \Phi_n(\delta) &= m, & \delta &= a^{\alpha'} b^{\beta'} \dots, & \alpha' &\leq \alpha, \beta' \leq \beta, \dots, \end{aligned}$$

the third formula being a generalization of Gauss' (4). If k is a fixed integer prime to m , $\Phi_n(m)$ is the number of sets of n integers $< m$ and prime to m such that each term of a set exceeds by k the preceding term modulo m . Consider the product P of the λ th terms of the $\Phi_n(m)$ sets. If $n=1$, $P \equiv \pm 1 \pmod{m}$ by Wilson's theorem. If $n > 1$,

$$P^{n-1} \equiv \{(-1)^{\lambda-1} k^{n-1} (\lambda-1)! (n-\lambda)!\} \Phi_n^{(m)} \pmod{m}.$$

For the case $k=\lambda=1$, $n=2$, we see that the product of those integers $< m$ and prime to m , which if increased by unity give integers prime to m , is $\equiv 1 \pmod{m}$.

E. Lucas¹⁹¹ gave a generalization of Schemmel's function, without mention of the latter. Let e_1, \dots, e_k be any integers. Let $\Psi(n)$ denote the number of those integers h , chosen from $0, 1, \dots, n-1$, such that

$$h - e_1, h - e_2, \dots, h - e_k$$

are prime to n . For $k < n$, $e_1 = 0, e_2 = -1, \dots, e_k = -(k-1)$, we have k consecutive integers $h, h+1, \dots, h+k-1$ each prime to n , and the number of such sets is $\Phi_k(n)$. Lucas noted that $\Psi(p)\Psi(q) = \Psi(pq)$ if p and q are relatively prime. Let $n = a^\alpha b^\beta \dots$, where a, b, \dots are distinct primes. Let λ be the number of distinct residues of e_1, \dots, e_k modulo a ; μ the number of their distinct residues modulo b ; etc. Then

$$\Psi(n) = a^{\alpha-1}(a-\lambda)b^{\beta-1}(b-\mu) \dots$$

L. Goldschmidt¹⁹² proved the theorems stated by Schemmel, and himself stated the further generalization: Select any $a-A$ positive integers $< a$, any $b-B$ positive integers $< b$, etc.; there are exactly

$$a^{\alpha-1}(a-A)b^{\beta-1}(b-B) \dots$$

integers $< m$ which are congruent modulo a to one of the $a-A$ numbers selected and congruent modulo b to one of the $b-B$ numbers selected, etc.

P. Bachmann¹⁹³ proved the theorems due to Schemmel and Lucas.

JORDAN'S GENERALIZATION OF EULER'S ϕ -FUNCTION.

C. Jordan,²⁰⁰ in connection with his study of linear congruence groups, proved that the number of different sets of k (equal or distinct) positive integers $\leq n$, whose g. c. d. is prime to n , is*

$$(10) \quad J_k(n) = n^k \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_q}\right)$$

¹⁹⁰Jour. für Math., 70, 1869, 191-2.

¹⁹¹Théorie des nombres, 1891, p. 402.

¹⁹²Zeitschrift Math. Phys., 39, 1894, 205-212.

¹⁹³Niedere Zahlentheorie, I, 1902, 91-94, 174-5.

²⁰⁰Traité des substitutions, Paris, 1870, 95-97.

*He used the symbol $[n, k]$. Several of the writers mentioned later used the symbol $\phi_k(n)$, which, however, conflicts with that by Thacker.¹⁵⁰

if p_1, \dots, p_q are the distinct prime factors of n . In fact, there are n^k sets of k integers $\leq n$, while $(n/p_1)^k$ of these sets have the common divisor p_1 , etc., whence

$$J_k(n) = n^k - \left(\frac{n}{p_1}\right)^k - \left(\frac{n}{p_2}\right)^k - \dots + \left(\frac{n}{p_1 p_2}\right)^k + \dots$$

Jordan noted the corollary: if n and n' are relatively prime,

$$(11) \quad J_k(nn') = J_k(n)J_k(n').$$

A. Blind¹⁵⁶ defined the function (10) also for negative values of k , proved (11), and the following generalization of (4):

$$(12) \quad \Sigma J_k(d) = n^k \text{ (} d \text{ ranging over the divisors of } n \text{)}.$$

W. E. Story²⁰¹ employed the symbol $\tau^k(n)$ for $J_k(n)$ and called it one of the two kinds of k th totients. The second kind is the number $\phi^k(n)$ of sets of k integers $\leq n$ and not all divisible by any factor of n , such that we do not distinguish between two sets differing only by a permutation of their numbers. He stated that

$$\phi^k(n) = \frac{1}{k!} \{ \tau^k(n) + t_1^k \tau^{k-1}(n) + t_2^k \tau^{k-2}(n) + \dots + t_{k-1}^k \tau(n) \},$$

where $1, t_1^k, t_2^k, \dots$ are the coefficients of the successive descending powers of x in the expansion of $(x+1)(x+2)\dots(x+k-1)$.

Story²⁰² defined "the k th totient of n to the condition κ to be the number of sets of k numbers $\leq n$ which satisfy condition κ . The number of sets of k numbers $\leq n$, all containing some common divisor of n satisfying the condition κ , but not all containing any one divisor of n satisfying the condition χ is (if different permutations of k numbers count as different sets)

$$n^k \frac{1}{\delta^k} \frac{1}{\delta'^k} \dots \left(1 - \frac{1}{\delta_1^k}\right) \left(1 - \frac{1}{\delta_1'^k}\right) \dots,$$

where δ, δ', \dots are the least divisors of n satisfying condition κ , while $\delta_1, \delta_1', \dots$ are the least divisors of n satisfying condition χ . Here a set of least divisors is a set of divisors no one of which is a multiple of any other."

E. Cesàro⁵⁷ (p. 345) stated that, if $\Phi_k(x)$ is the number of sets of k integers $\leq x$ whose g. c. d. is prime to x , then

$$\Sigma \Phi_k(d) = \binom{n+k-1}{k}, \quad \Phi_k(n) = \binom{J+k-1}{k},$$

where J^s is to be replaced by $J_s(n)$, and d ranges over the divisors of n .

J. W. L. Glaisher²⁰³ proved (12) by means of a symbolic expression for the infinite series $\Sigma J_k(n)f(x^n)$. If $\mu(n)$ is Merten's function,

$$J_k(n) - \Sigma p_1^k J_k\left(\frac{n}{p_1}\right) + \Sigma p_1^k p_2^k J_k\left(\frac{n}{p_1 p_2}\right) - \dots = \mu(n),$$

where the summations relate to the distinct prime factors p_i of n . Using

²⁰¹Johns Hopkins University Circulars, 1, 1881, 132.

²⁰²*Ibid.*, p. 151. Cf. Amer. Jour. Math., 3, 1880, 382-7.

²⁰³London, Ed. Dublin Phil. Mag., (5), 18, 1884, 531, 537-8.

these formulas for $n=1, 2, \dots, n$, we obtain two determinants of order n , each equal to $(-1)^{n-1}J_k(n)$:

$$\begin{vmatrix} 1^k & 2^k & 3^k & 4^k & \dots \\ 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 1 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{vmatrix}, \quad \begin{vmatrix} 1 & -1 & -1 & 0 & -1 & 1 & \dots \\ 1 & -2^k & -3^k & 0 & -5^k & 6^k & \dots \\ 0 & 1^k & 0 & -2^k & 0 & -3^k & \dots \\ 0 & 0 & 1^k & 0 & 0 & -2^k & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}.$$

L. Gegenbauer²⁰⁴ proved (12). For $n=p_1^{\nu_1} \dots p_q^{\nu_q}$, set

$$\pi(n) = (-1)^q p_1 \dots p_q, \quad \lambda(n) = (-1)^{\nu_1 + \dots + \nu_q},$$

$$F(d) = (-1)^{(k+1)w(r/d)} \pi^k \left(\frac{r}{d} \right) J_k \left(\frac{r}{d} \right),$$

where $w(n)$ denotes the number of distinct prime factors of n . By means of the series $\zeta(s) = \sum n^{-s}$, he proved that, when d ranges over the divisors of r ,

$$\sum F(d) d^{2k} = r^k, \quad \sum F(d) d^{3k} = r^k \sum d^k J_k(d),$$

$$\sum F(d) J_k(d) d^k = 0, \quad \sum (-1)^{(k+1)w(r/d)} d^k \pi^k \left(\frac{r}{d} \right) = 0,$$

the last holding if r has no square factor and following from the third in view of (11),

$$J_k(r) = \sum d \mu \left(\frac{r}{d} \right), \quad \sum F(d) d^k \mu(d) = r^{2k} \mu(r), \quad \sum \lambda(d) J_k(d) J_k \left(\frac{r}{d} \right) = 0 \text{ or } J_{2k}(\sqrt{r}),$$

according as r is or is not a square,

$$\sum_{m, n} (-1)^{(k+1)w(m)} \pi^k(m) J_k(m) J_{2k}(n) n^{2k} = r^k \lambda(r) J_k(r) \quad (mn^2 = r),$$

$$\sum F(d) J_{k+t}(d) d^k = r^{k+t} J_k(r), \quad \sum d^t J_k(d) J_t \left(\frac{r}{d} \right) = J_{k+t}(r) \quad (t > 0),$$

$$\sum J_k(n_1) \dots J_k(n_t) n_1^{(t-1)k} n_2^{(t-2)k} \dots n_{t-1}^k = r^{tk},$$

where n_1, \dots, n_t range over all sets of solutions of $n_1 n_2 \dots n_{t+1} = n$, the case $k=1$ being due to H. G. Cantor.⁴⁹

E. Cesàro¹⁶⁹ derived (10) from (12), writing ζ_{1-k} for J_k .

E. Cesàro²⁰⁵ denoted $J_k(n)$ by $\psi^k(n)$ and gave (12).

L. Gegenbauer¹⁷⁰ gave the further generalization

$$\sum_{x=1}^n (g_p(x))^k = \sum_{x=1}^{\nu} \left[\frac{n}{x^p} \right] J_k(x), \quad \nu = [\sqrt[p]{n}].$$

J. Hammond²⁰⁶ wrote $\psi(n, d)$ for $\sum f(\delta)$, where f is an arbitrary function and δ ranges over all multiples $\leq n$ of the fixed divisor d of n . Then

$$(13) \quad \sum f(t) = \psi(n, 1) - \sum \psi(n, p_1) + \sum \psi(n, p_1 p_2) - \dots,$$

²⁰⁴Sitzungsber. Ak. Wiss. Wien (Math.), 89 II, 1884, 37-46. Cf. p. 841. See Gegenbauer⁷² of Ch. X.

²⁰⁵Annali di Mat., (2), 14, 1886-7, 142-6.

²⁰⁶Messenger Math., 20, 1890-1, 182-190.

where t ranges over the integers $\leq n$ which are prime to n , while p_1, p_2, \dots denote the distinct prime factors of n . If $f(t) \equiv 1$, then $\psi(n, d) = n/d$ and (13) becomes

$$\phi(n) = n - \sum \frac{n}{p_1} + \sum \frac{n}{p_1 p_2} - \dots = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots$$

Next, take $f(t) = a_0 + a_1 t + a_2 t^2 + \dots$. Using hyperbolic functions,

$$\Sigma f(t) = \frac{1}{2} \coth(z/2) = \frac{1}{z} + \frac{z}{12} - \frac{z^3}{720} + \dots,$$

provided z' be replaced by $n'f_r(n)J_{-r}(n)$, where

$$f_1(n) = f'(n) - a_1, \quad f_2(n) = f''(n) - 2a_2, \dots, \quad f_{-1}(n) = \int f(n) dn.$$

Hence, since $J_1(n) = \phi(n)$,

$$\Sigma f(t) = \frac{\phi(n)}{n} f_{-1}(n) + \frac{n}{12} J_{-1}(n) f_1(n) - \frac{1}{720} n^3 J_{-3}(n) f_3(n) + \dots$$

In particular, for $f(t) = t^k$, we get $\phi_k(n)$. In Prouhet's¹⁸ first formula, δ may be replaced by the g. c. d. $\Delta_{a,b}$ of a and b . The generalization

$$J_k(ab) = J_k(a) J_k(b) \frac{\Delta_{a,b}^k}{J_k(\Delta_{a,b})}$$

is proved. From (12) we get by addition*

$$(14) \quad \sum_{j=1}^n \left[\frac{n}{j} \right] J_k(j) = 1^k + 2^k + \dots + n^k.$$

Taking $n=1, 2, \dots, n$, we obtain equations whose solution gives $J_k(n)$ expressed as a determinant of order n in which the elements of the last column are $1, 1+2^k, 1+2^k+3^k, \dots$, while for $s < n$ the s th column consists of $s-1$ zeros followed by s units, then s twos, etc. For $s > 0$, the element in the $(s+1)$ th row and r th column in Glaisher's²⁰³ first determinant is 1 or 0 according as r/s is integral or fractional.

J. Vályi²⁰⁷ used $J_2(n) \div \phi(n)$ in his enumeration of the n -fold perspective polygons of n sides inscribed in a cubic curve.

H. Weber²⁰⁸ proved (10) for $k=2$.

L. Carlini²⁰⁹ gave without references (10), (11), (12), with $\phi\left(\frac{k}{n}\right)$ for $J_n(k)$.

E. Cesàro²¹⁰ noted that (12) implies (10). For, if $\Sigma f(d) = F(n)$, we have by inversion (Ch. XIX), $f(n) = \Sigma \mu(d) F(n/d)$. The case $f = J_l$ gives

$$\frac{J_l(n)}{n^l} = \Sigma \frac{\mu(d)}{d^l}.$$

The latter is a case of $G(n) = \Sigma g(d)$ and hence, with (12) and

$$\Sigma f(d) G\left(\frac{n}{d}\right) \equiv \Sigma g(d) F\left(\frac{n}{d}\right),$$

*This work, *Mess. Math.*, 20, 1890-1, p. 161, for $k=1$, is really due to Dirichlet.²¹ Formula (14) is the case $\rho=1$ of Gegenbauer's, p. 217.

²⁰⁷*Math. Nat. Berichte aus Ungarn*, 9, 1890, 148; 10, 1891, 171.

²⁰⁸*Elliptische Functionen*, 1891, 225; ed. 2, 1908 (*Algebra III*), 215.

²⁰⁹*Periodico di Mat.*, 6, 1891, 119-122.

²¹⁰*Ibid.*, 7, 1892, 1-6.

yields

$$\sum J_k(d) J_l\left(\frac{n}{d}\right) \left(\frac{d}{n}\right)^l = \sum \frac{\mu(d)}{d^l} \left(\frac{n}{d}\right)^k = n^k \frac{J_{l+k}(n)}{n^{l+k}},$$

or

$$J_{l+k}(n) = \sum d^l J_k(d) J_l\left(\frac{n}{d}\right),$$

which is next to the last formula of Gegenbauer's.²⁰⁴ Similarly,

$$\sigma_{l+k}(n) = \sum d^k J_l(d) \sigma_k\left(\frac{n}{d}\right),$$

which is the case $t=1$ of Gegenbauer's⁷² fifth formula in Ch. X, $\sigma_k(n)$ being the sum of the k th powers of the divisors of n .

E. Weyr²¹¹ interpreted $J_2(n)$ in connection with involutions on loci of genus 1. From the same standpoint, L. Gegenbauer²¹² proved (12) for $k=2$ and noted that the value (10) of $J_2(n)$ then follows by the usual method of number-theoretic derivatives.

L. Gegenbauer^{212a} wrote $\phi_k(m, n)$ for the number of sets of k positive integers $\leq m$ whose g. c. d. is prime to $n = p_1^{a_1} \dots p_r^{a_r}$ and proved a formula including

$$[m]^k = \phi_k(m, n) + \sum_{\sigma=1}^r \sum_{\lambda_1, \dots, \lambda_\sigma=1}^r (\lambda_1, \dots, \lambda_\sigma)^2 \phi_k\left(\frac{m}{p_{\lambda_1} \dots p_{\lambda_\sigma}}, \frac{n}{p_{\lambda_1}^{a_{\lambda_1}} \dots p_{\lambda_\sigma}^{a_{\lambda_\sigma}}}\right),$$

where $(\lambda_1, \dots, \lambda_\sigma)$ is the determinant derived from that with unity throughout the main diagonal and zeros elsewhere by replacing the γ th row by the λ_γ th row for $\gamma=1, \dots, \sigma$. The case $m=n$, $k=1$, is due to Pepin.³⁷ There is an analogous formula involving the sum of the k th powers of the positive integers $\leq m$ and prime to n .

E. Jablonski⁷⁴ used $J_k(n)$ in connection with permutations.

G. Arnoux²¹³ proved (10) in connection with modular space.

*J. J. Tschistakow²¹⁴ (or Cistiakov) treated the function $J_k(n)$.

R. D. von Sterneck²¹⁵ proved that

$$J_k(n) = \sum J_r(\lambda_1) J_{k-r}(\lambda_2) = \sum \phi(\lambda_1) \dots \phi(\lambda_k),$$

the λ 's ranging over all sets of integers $\leq n$ whose l. c. m. is n . To generalize this, let $J_k(n; m_1, \dots, m_k)$ be the number of sets of integers i_1, \dots, i_k , whose g. c. d. is prime to n , while $i_j \leq n/m_j$ for $j=1, \dots, k$. Then

$$\begin{aligned} J_k(n; m_1, \dots, m_k) &= \sum J_r(\lambda_1; m'_1, \dots, m'_r) J_{k-r}(\lambda_2; m'_{r+1}, \dots, m'_k) \\ &= \sum J_1(\lambda_1; m_1) \dots J_1(\lambda_k; m_k), \end{aligned}$$

the λ 's ranging over all sets of integers $\leq n$ whose l. c. m. is n , while m'_1, \dots, m'_k form any fixed permutation of m_1, \dots, m_k , and $J_1(n; m)$, designated $\phi^{(m)}(n)$ by the author, is the number of integers $\leq n/m$ which are prime to n . Also,

²¹¹Sitzungsberichte Ak. Wiss. Wien (Math.), 101, IIa, 1892, 1729-1741.

²¹²Monatshefte Math. Phys., 4, 1893, 330.

^{212a}Denkschr. Ak. Wiss. Wien (Math.), 60, 1893, 25-47.

²¹³Arithmétique graphique; espaces arith. hypermagiques, 1894, 93.

²¹⁴Math. Soc. Moscow, 17, 1894, 530-7 (in Russian).

²¹⁵Monatshefte Math. Phys., 5, 1894, 255-266.

$$\Sigma J_k(d; m_1, \dots, m_k) = \left[\frac{n}{m_1} \right] \left[\frac{n}{m_2} \right] \dots \left[\frac{n}{m_k} \right],$$

where d ranges over the divisors of n , the case $k=1$ being due to Laguerre.³⁵ In the latter case, take $n=1, \dots, n$ and add. Thus

$$\sum_{k=1}^n J_1(k; m) \left[\frac{n}{k} \right] = \sum_{j=1}^n \left[\frac{j}{m} \right] = \frac{1}{2} \left\{ \frac{n^2}{m} + \frac{n}{m} - n + \left(n, \frac{n}{m} \right) \right\},$$

the last equality, in which (n, b) is the g. c. d. of n, b , following from expressions for (n, b) given by Hacks⁴² of Ch. XI. In the present paper the above double equation was proved geometrically. For $m=1$, we get Dirichlet's²¹ formula. The g. c. d. of three numbers is expressed in terms of them and $[x]$.

The initial formulas were proved geometrically, but were recognized to be special cases of a more general theorem. Let

$$\Sigma f_i(d) = F_i(n) \quad (i=1, \dots, k),$$

where d ranges over all divisors of n . Then the function

$$\psi(n) = \Sigma f_1(\lambda_1) \dots f_k(\lambda_k) \quad (\text{l. c. m. of } \lambda_1, \dots, \lambda_k \text{ is } n)$$

has the property

$$\Sigma \psi(d) = F_1(n) \dots F_k(n).$$

Hence in the terminology of Bougaief (Ch. XIX) the number-theoretic derivative $\psi(n)$ of $F_1(n) \dots F_k(n)$ equals the sum of the products of the derivatives f_i of the factors F_i , the arguments ranging over all sets of k numbers having n as their g. c. d.

L. Gegenbauer^{215a} proved easily that, if $[n, \dots, t]$ is the g. c. d. of n, \dots, t

$$\sum_{x_1, \dots, x_s=1}^n F([n, x_1, \dots, x_s]) = \Sigma F(d) J_s \left(\frac{n}{d} \right),$$

where d ranges over all divisors of n , and F is any function.

K. Zsigmondy²¹⁶ considered any abelian (commutative) group G with the independent generators g_1, \dots, g_s of periods n_1, \dots, n_s , respectively. Any element $g_1^{h_1} \dots g_s^{h_s}$ of G is of period δ if and only if δ is the least positive value of x for which xh_1, \dots, xh_s are multiples of n_1, \dots, n_s , respectively. The number of elements of period δ of G is thus the number of sets of positive integers h_1, \dots, h_s ($h_1 \leq n_1, \dots, h_s \leq n_s$) such that δ is the least value of x for which xh_1, \dots, xh_s are divisible by n_1, \dots, n_s , respectively. The number of sets is shown to be

$$\psi(\delta; n_1, \dots, n_s) = \prod_{j=1}^s \delta_j \prod_{i=1}^r (1 - 1/q_i^{l_i}),$$

where δ_j is the g. c. d. of δ and n_j ; q_1, \dots, q_r are the distinct prime factors of δ ; while l_i is the number of those integers n_1, \dots, n_s which contain q_i at least as often as δ contains it. If δ and δ' are relatively prime,

$$\psi(\delta; n_1, \dots, n_s) \psi(\delta'; n_1, \dots, n_s) = \psi(\delta\delta'; n_1, \dots, n_s).$$

^{215a}Sitzungsber. Akad. Wiss. Wien (Math.), 103, IIa, 1894, 115.

²¹⁶Monatshefte Math. Phys., 7, 1896, 227-233. For his ϕ we write ψ , as did Carmichael.²¹

If d ranges over all divisors of the product $n_1 \dots n_s$,

$$\sum_d \psi(\delta; n_1, \dots, n_s) = n_1 n_2 \dots n_s.$$

In case δ divides each n_i ($i=1, \dots, s$), ψ becomes Jordan's $J_s(\delta)$.

As a generalization (pp. 237-9) consider sets of positive integers a_1, \dots, a_s , where $a_j = 1, 2, \dots, \gamma_j$ for $j=1, 2, \dots, s$. Counting the sets not of the form

$$n_i^{(1)} a_1, n_i^{(2)} a_2, \dots, n_i^{(s)} a_s \quad (i=1, \dots, r),$$

we get the number

$$\prod_{j=1}^s \gamma_j - \sum_i \prod_{j=1}^s \left[\frac{\gamma_j}{n_i^{(j)}} \right] + \sum_{i, i'} \prod_{j=1}^s \left[\frac{\gamma_j}{(n_i^{(j)}, n_{i'}^{(j)})} \right] - \dots$$

where (n_1, n_2, \dots) is the l. c. m. of n_1, n_2, \dots . In particular, take

$$n_i^{(1)} = \dots = n_i^{(s)} = n_i \quad (i=1, \dots, r),$$

where n_1, \dots, n_r are relatively prime in pairs, and let N be a positive multiple of n_1, \dots, n_r such that

$$N < m_j, \quad \frac{N}{\gamma} \geq m_j > \frac{N}{1 + \gamma_j} \quad (j=1, \dots, s).$$

Then the above expression equals

$$J_s'(N; m_1, \dots, m_s) = \prod_{j=1}^s \left[\frac{N}{m_j} \right] - \sum_i \prod_{j=1}^s \left[\frac{N}{m_j n_i} \right] + \sum_{i, i'} \prod_{j=1}^s \left[\frac{N}{m_j n_i n_{i'}} \right] - \dots,$$

which determines the number of sets

$$a_1, \dots, a_s \quad (a_j = 1, 2, \dots, \left[\frac{N}{m_j} \right]; j=1, \dots, s)$$

whose g. c. d. is divisible by no one of n_1, n_2, \dots, n_s . By inversion,

$$\sum J_s' \left(\frac{N}{d}; m_1, \dots, m_s \right) = \prod_{j=1}^s \left[\frac{N}{m_j} \right],$$

where d ranges over the divisors of N which are products of powers of n_1, \dots, n_r . When n_1, \dots, n_s are the distinct prime factors of N , $J_s'(N; m_1, \dots, m_s)$ becomes the function $J_s(N; m_1, \dots, m_s)$ of von Sterneck.²¹⁵ As in the case of the latter function, we have

$$J_s'(N; m_1, \dots, m_s) = \sum J_1'(\lambda_1; m_1) \dots J_1'(\lambda_s; m_s),$$

the λ 's ranging over all sets whose l. c. m. is N .

L. Carlini²¹⁷ proved that if a ranges over the integers for which $[2n/a] = 2k+1$, then

$$\sum J_k(a) = s_{2n}^{(k)} - 2s_n^{(k)}, \quad s_m^{(k)} \equiv 1^k + \dots + m^k.$$

For $k=1$, this becomes $\sum \phi(a) = n^2$ [E. Cesàro, p. 144 of this History].

D. N. Lehmer²¹⁸ called $J_m(n)$ the m -fold totient of n or multiple totient of n of multiplicity m . He proved that, if $k = p_1^{a_1} \dots p_r^{a_r}$,

$$J_m(k^n) = k^{m(n-1)} J_m(k), \quad J_m(ky) = J_m(y) \prod_{i=1}^r \{ p_i^{m a_i} - p_i^{m(a_i-1)} \lambda(y, p_i) \},$$

where $\lambda(y, p_i) = 0$ or 1 according as p_i is or is not a divisor of y . In the

²¹⁷Periodico di Mat., 12, 1897, 137-9.

²¹⁸Amer. Jour. Math., 22, 1900, 293-335.

second formula the product equals the similar function of y' if y and y' are congruent modulo $p_1 p_2 \dots p_r$. Consider the function

$$\Phi_m(x, n, k) = \sum_{i=1}^{[x/k]} J_m(i^n k^n),$$

where m, n, k are positive integers and x is a positive number. Then if $S(x, k)$ denotes $1^k + 2^k + \dots + [x]^k$, it is proved that

$$\sum_{j=1}^{[x]} j^{m(n-1)} \Phi_m\left(\frac{x}{j}, n, 1\right) = S(x, mn),$$

which for $m=n=1$ becomes Sylvester's⁵⁵ formula. By inversion,

$$\Phi_m(x, n, 1) = \sum_{i=1}^{[x]} \mu(i) i^{m(n-1)} S\left(\frac{x}{i}, mn\right),$$

where $\mu(i)$ is Merten's function. For k as above and $k' = k/p_r^{ar}$,

$$\begin{aligned} \Phi_m(x, n, k) &= p_r^{m(ar-1)} \left\{ (p_r - 1) \Phi_m\left(\frac{x}{p_r^{ar}}, n, k'\right) + \Phi_m\left(\frac{x}{p_r^{ar}}, n, p_r k'\right) \right\} \\ &= p_r^{m(ar-1)} (p_r - 1) \sum_{j=0}^l p_r^{m(n-1)j} \Phi_m\left(\frac{x}{p_r^{ar+j}}, n, k'\right), \end{aligned}$$

where l is the least value of j for which $[x/p_r^{ar+j}] = 0$. Hence $\Phi_m(x, n, k)$ can be expressed in terms of functions $\Phi_m(y, n, 1)$. True relations are derived from the last four equations by replacing n by $1-n$ and $\Phi_m(x, 1-n, k)$ by

$$\Omega_m(x, n, k) = \sum_{i=1}^{[x/k]} J_m(ik) \cdot (ik)^{-nm}.$$

Proof is given of the asymptotic formula

$$\Phi_m(x, n, k) = \frac{x^{mn+1}}{mn+1} \frac{P_{m,k}}{D_{m+1}} + \epsilon, \quad |\epsilon| \leq Ax^{mn} \log x,$$

where A is finite and independent of x, m, n , while

$$D_{m+1} = \sum_{j=1}^{\infty} \frac{1}{j^{m+1}}, \quad P_{m,k} = \prod_{i=1}^r \frac{p_i - 1}{p_i^{a_i-1} (p_i^{m+1} - 1)}, \quad P_{m,1} = 1.$$

For $m=n=k=1$, this result becomes that of Mertens³⁶ (and Dirichlet²¹). The asymptotic expressions found for $\Omega_m(x, n, k)$ are different for the cases $n=1, n=2, n>2$.

A set of m integers (not necessarily positive) having no common divisor >1 is said to define a totient point. Let one coordinate, as x_m , have a fixed integral value $\neq 0$, while x_1, \dots, x_{m-1} take integral values such that $[x_1/x_m], \dots, [x_{m-1}/x_m]$ have prescribed values; we obtain a compartment in space of m dimensions which contains $J_{m-1}(x_m)$ totient points. For example, if $m=3, x_3=6$, and the two prescribed values are zero, there are 24 totient points $(x_1, x_2, 6)$ for which $0 \leq x_1 < 6, 0 \leq x_2 < 6$, while x_1 and x_2 have no common divisor dividing 6. For $x_1=1$ or 5, x_2 has 6 values; for $x_1=2$ or 4, $x_2=1, 3$ or 5; for $x_1=3, x_2=1, 2, 5$; for $x_1=0, x_2=0, 1, 5$.

Given a closed curve $r=f(\theta)$, decomposable into a finite number of segments for each of which $f(\theta)$ is a single-valued, continuous function. Let

K be the area of the region bounded by this curve, and N the number of points (x, y) within it or on its boundary such that x is a multiple of k and is prime to y . Then

$$\lim_{k \rightarrow \infty} \frac{N}{K} = \frac{6}{\pi^2} P_{1, k},$$

where K increases by uniform stretching of the figure from the origin.

In particular, consider the number N of irreducible fractions $x/y \leq 1$ whose denominators are $\leq n$. Since $x \leq y$, the area K of the triangular region is $n^2/2$. Hence $N = (n^2/2)(6/\pi^2)$, approximately (Sylvester⁵⁵). Again, the number of irreducible fractions whose numerators lie between l and $l+m$, and denominators between l' and $l'+m'$, is $6mm'/\pi^2$, approximately.

There is a similar theorem in which the points are such that y is divisible by k' , while three new constants obey conditions of relative primality to each other or to x, y, k, k' .

Extensions are stated for m -dimensional space.

E. Cahen²¹⁹ called $J_k(n)$ the indicateur of k th order of n .

G. A. Miller²²⁰ evaluated $J_k(m)$ by noting that it is the number of operators of period m in the abelian group with k independent generators of period m .

G. A. Miller²²¹ proved (10) and (11) by using the same abelian group.

E. Busche²²² indicated a proof of (10) and (12) by an extension to space of $k+1$ dimensions of Kronecker's²²³ plane, in which every point whose rectangular coordinates x, y are integers is associated with the g. c. d. of x, y .

A. P. Minin²²⁴ proved (14) and some results due to Gegenbauer.²⁰⁴

R. D. Carmichael²²⁵ gave a simple proof of Zsigmondy's²¹⁶ formula for ψ .

G. Métrod²²⁶ stated that the number of incongruent sets of solutions of $xy' - x'y \equiv a \pmod{m}$ is $\sum dm J_2(m/d)$, where d ranges over the common divisors of m and a . When a takes its m values, the total number of sets of solutions is

$$m^4 = \sum_{D: m} \phi\left(\frac{m}{D}\right) \sum_{d: D} dm J_2\left(\frac{m}{d}\right).$$

It is asked if like relations hold for $J_k, k > 2$.

Cordone⁹¹ and Sanderson¹¹⁵ (of Ch. VIII) used Jordan's function in giving a generalization of Fermat's theorem to a double modulus.

FAREY SERIES.

Flitcon²⁴⁸ gave the number of irreducible fractions < 1 with each denominator < 100 , stating in effect the value of Euler's $\phi(n)$ when n is a product of four or fewer primes.

²¹⁹Théorie des nombres, 1900, p. 36; I, 1914, 396-400.

²²⁰Amer. Math. Monthly, 11, 1904, 129-130.

²²¹Amer. Jour. Math., 27, 1905, 321-2.

²²²Math. Annalen, 60, 1905, 292.

²²³Vorlesungen über Zahlentheorie, 1901, I, p. 242.

²²⁴Matem. Sbornik (Moscow Math. Soc.), 27, 1910, 340-5.

²²⁵Quart. Jour. Math., 44, 1913, 94-104.

²²⁶L'intermédiaire des math., 20, 1913, 148. Proof, Sphinx-Oedipe, 9, 1914, 4.

²⁴⁸Ladies' Diary, 1751. Reply to Question 281, 1747-8. T. Leybourn's Math. Quest. proposed in Ladies' Diary, 1, 1817, 397-400.

C. Haros²⁴⁹ proved the results rediscovered by Farey²⁵⁰ and Cauchy.²⁵²

J. Farey²⁵⁰ stated that if all the proper vulgar fractions in their lowest terms, having both numerator and denominator not exceeding a given number n , be arranged in order of magnitude, each fraction equals a fraction whose numerator and denominator equal respectively the sum of the numerators and sum of the denominators of the two fractions adjacent to it in the series. Thus, for $n=5$, the series is

$$\frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5},$$

and

$$\frac{1}{4} = \frac{1+1}{5+3}, \quad \frac{2}{5} = \frac{1+1}{3+2}.$$

Henry Goodwyn mentioned this property on page 5 of the introduction to his "tabular series of decimal quotients" of 1818, published in 1816 for private circulation (see Goodwyn,^{21, 22} Ch. VI), and is apparently to be credited with the theorem. It was ascribed to Goodwyn by C. W. Merrifield.²⁵¹

A. L. Cauchy²⁵² proved that, if a/b , a'/b' , a''/b'' are any three consecutive fractions of a Farey series, b and b' are relatively prime and $a'b - ab' = 1$ (so that $a'/b' - a/b = 1/bb'$). Similarly, $a''b' - a'b'' = 1$, so that $a + a' : b + b'' = a' : b'$, as stated by Farey.

Stouvenel²⁵³ proved that, in a Farey series of order n , if two fractions a/b and c/b are complementary (i. e., have the sum unity), the same is true of the fraction preceding a/b and that following c/b . The two fractions adjacent to $1/2$ are complementary and their common denominator is the greatest odd integer $\leq n$. Hence $1/2$ is the middle term of the series and two fractions equidistant from $1/2$ are complementary. To find the third of three consecutive fractions a/b , a'/b' , x/y , we have $a+x = a'z$, $b+y = b'z$ (Farey), and we easily see that z is the greatest integer $\leq (n+b)/b'$.

M. A. Stern²⁵⁴ studied the sets m , n , and m , $m+n$, n , and m , $2m+n$, $m+n$, $m+2n$, n , etc., obtained by interpolating the sum of consecutive terms. G. Eisenstein^{254a} briefly considered such sets.

*A. Brocot²⁵⁵ considered the sets obtained by mediation [Farey] from $0/1$, $1/0$:

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{0}; \quad \frac{0}{1}, \frac{1}{2}, \frac{1}{1}, \frac{2}{1}, \frac{1}{0}; \dots$$

Herzer²⁵⁶ and Hrabak²⁵⁷ gave tables with the limits 57 and 50.

G. H. Halphen²⁵⁸ considered a series of irreducible fractions, arranged in order of magnitude, chosen according to a law such that if any fraction f is excluded then also every fraction is excluded if its two terms are at least

²⁴⁹Jour. de l'école polyt., cah. 11, t. 4, 1802, 364-8.

²⁵⁰Philos. Mag. and Journal, London, 47, 1816, 385-6; [48, 1816, 204]; Bull. Sc. Soc. Philomatique de Paris, (3), 3, 1816, 112.

²⁵¹Math. Quest. Educat. Times, 9, 1868, 92-5.

²⁵²Bull. Sc. Soc. Philomatique de Paris, (3), 3, 1816, 133-5. Reproduced in Exercices de Math., 1, 1826, 114-6; Oeuvres, (2), 6, 1887, 146-8.

²⁵³Jour. de mathématiques, 5, 1840, 265-275.

²⁵⁴Jour. für Math., 55, 1858, 193-220.

^{254a}Bericht Ak. Wiss. Berlin, 1850, 41-42.

²⁵⁵Calcul des rouages par approximation, Paris, 1862. Lucas.²⁵⁷

²⁵⁶Tabellen, Basle, 1864.

²⁵⁷Tabellen-Werk, Leipzig, 1876.

²⁵⁸Bull. Soc. Math. France, 5, 1876-7, 170-5.

equal to the corresponding terms of f . Such a series has the properties noted by Farey and Cauchy for Farey series.

E. Lucas²⁵⁹ considered series 1, 1 and 1, 2, 1, etc., formed as by Stern. For the n th series it is stated that the number of terms is $2^{n-1}+1$, their sum is $3^{n-1}+1$, the greatest two terms (of rank $2^{n-2}+1 \pm 2^{n-1}$) are

$$\frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}.$$

Changing n to p , we obtain the value of certain other terms.

J. W. L. Glaisher²⁶⁰ gave some of the above facts on the history of Farey series. Glaisher²⁶¹ treated the history more fully and proved (p. 328) that the properties noted by Farey and Cauchy hold also for the series of irreducible fractions of numerators $\leq m$ and denominators $\leq n$.

Edward Sang²⁶² proved that any fraction between A/a and C/γ is of the form $(pA+qC)/(p\alpha+q\gamma)$, where p and q are integers, and is irreducible if p, q are relatively prime.

A. Minine²⁶³ considered the number $S(a, N)$ of irreducible fractions a/b such that $b+aa \leq N$. Let $\phi(b)_p$ denote the number of integers $\leq p$ which are prime to b . Then, for $a > 0$,

$$S(a, N) = \sum_{b=1}^{N-a} \phi(b)_p, \quad p = \left[\frac{N-b}{a} \right],$$

since for each denominator b there are $\phi(b)_p$ integers prime to b for which $b+aa \leq N$ and hence that number of fractions.

A. F. Pullich²⁶⁴ proved Farey's theorem by induction, using continued fractions.

G. Airy²⁶⁵ gave the 3043 irreducible fractions with numerator and denominator ≤ 100 .

J. J. Sylvester²⁶⁶ showed how to deduce the number of fractions in a Farey series by means of a functional equation.

Sylvester,^{55, 56} Cesàro,⁶⁵ Vahlen,⁸³ Axer,¹¹⁵ and Lehmer²¹⁸ investigated the number of fractions in a Farey series.

Sylvester^{266a} discussed the fractions x/y for which $x < n, y < n, x+y \leq n$.

M. d'Ocagne²⁶⁷ prolonged Farey's series by adding $1/1$ in the p th place, where $p = \phi(1) + \dots + \phi(n)$. From the first p terms we obtain the next p by adding unity, then the next p by adding unity, etc. Consider a series $S(a, N)$ of irreducible fractions a_i/b_i in order of magnitude such that $b_i + aa_i \leq N$, where a is any fixed integer called the characteristic. All the series $S(a, N)$ with a given base N may be derived from Farey's series

²⁵⁹Bull. Soc. Math. France, 6, 1877-8, 118-9.

²⁶⁰Proc. Cambr. Phil. Soc., 3, 1878, 194.

²⁶¹London Ed. Dub. Phil. Mag., (5), 7, 1879, 321-336.

²⁶²Trans. Roy. Soc. Edinburgh, 28, 1879, 287.

²⁶³Jour. de math. élém. et spéc., 1880, 278. Math. Soc. Moscow, 1880.

²⁶⁴Mathesis, 1, 1881, 161-3.

²⁶⁵Trans. Inst. Civil Engineers; cf. Phil. Mag., 1881, 175.

²⁶⁶Johns Hopkins Univ. Circulars, 2, 1883, 44-5, 143; Coll. Math. Papers, 3, 672-6, 687-8.

^{266a}Amer. Jour. Math., 5, 1882, 303-7, 327-330; Coll. Math. Papers, IV, 55-9, 78-81.

²⁶⁷Annales Soc. Sc. Bruxelles, 10, 1885-6, II, 90. Extract in Bull. Soc. Math. France, 14, 1885-6, 93-7.

$S(0, N)$ by use of

$$a_i(a, N) = a_i(0, N), \quad b_i(a, N) = b_i(0, N) - aa_i(0, N).$$

Thus $a_i b_{i-1} - a_{i-1} b_i = 1$, so that the area of $OA_i A_{i-1}$ is $1/2$ if the point A_i has the coordinates a_i, b_i . All points representing terms of the same rank in all the series of the same base lie at equally spaced intervals on a parallel to the x -axis, and the distance between adjacent points is the number of units between this parallel and the x -axis.

A. Hurwitz²⁶⁸ applied Farey series to the approximation of numbers by rational fractions and to the reduction of binary quadratic forms.

J. Hermes²⁶⁹ designated as numbers of Farey the numbers $\tau_1 = 1, \tau_2 = 2, \tau_3 = \tau_4 = 3, \tau_5 = 4, \tau_6 = \tau_7 = 5, \tau_8 = 4, \dots$ with the recursion formula

$$\tau_n = \tau_{n-2^v} + \tau_{2^v+1-n+1}, \quad 2^v < n \leq 2^{v+1},$$

and connected with the representation of numbers to base 2. The ratios of the τ 's give the Farey fractions.

K. Th. Vahlen^{269a} noted that the formation of the convergents to a fraction w by Farey's series coincides with the development of w into a continued fraction whose numerators are $\neq 1$, and made an application to the composition of linear fractional substitutions.

H. Made²⁷⁰ applied Hurwitz's method to numbers $a + bi$.

E. Busche²⁷¹ applied geometrically the series of irreducible fractions of denominators $\leq a$ and numerators $\leq b$, and noted that the properties of Farey series ($a = b$) hold [Glaisher²⁶¹].

W. Sierpinski²⁷² used consecutive fractions of Farey series of order m to show that, if x is irrational,

$$\lim_{x \rightarrow \infty} \left\{ \sum_{k=1}^n [kx] - \frac{xn(n+1)}{2} + \frac{n}{2} \right\} = 0.$$

Expositions of the theory of Farey series were given by E. Lucas,²⁷³ E. Cahen,²⁷⁴ Bachmann.²⁷⁵

An anonymous writer,²⁷⁶ starting with the irreducible fractions < 1 , arranged in order of magnitude, with the denominators ≤ 10 , inserted the fractions with denominator 11 by listing the pairs of fractions $0/1, 1/10; 1/6, 1/5; 1/4, 2/7; \dots$, the sum of whose denominators is 11, and noting that between the two of each pair lies a fraction with denominator 11 and numerator equal the sum of their numerators.

²⁶⁸Math. Annalen, 44, 1894, 417-436; 39, 1891, 279; 45, 1894, 85; Math. Papers of the Chicago Congress, 1896, 125. Cf. F. Klein, *Ausgewählte Kapitel der Zahlentheorie*, I, 1896, 196-210. Cf. G. Humbert, *Jour. de Math.*, (7), 2, 1916, 116-7.

²⁶⁹Math. Annalen, 45, 1894, 371. Cf. L. von Schrutka, 71, 1912, 574, 583.

^{269a}Jour. für Math., 115, 1895, 221-233.

²⁷⁰Ueber Fareysche Doppelreihen, Diss. Giessen, Darmstadt, 1903.

²⁷¹Math. Annalen, 60, 1905, 288.

²⁷²Bull. Inter. Acad. Sc. Cracovie, 1909, II, 725-7.

²⁷³Théorie des nombres, 1891, 467-475, 508-9.

²⁷⁴Éléments de la théorie des nombres, 1900, 331-5.

²⁷⁵Niedere Zahlentheorie, 1, 1902, 121-150; 2, 1910, 55-96.

²⁷⁶Zeitschrift Math. Naturw. Unterricht, 45, 1914, 559-562.

CHAPTER VI.

PERIODIC DECIMAL FRACTIONS; PERIODIC FRACTIONS; FACTORS OF $10^n \pm 1$.

Ibn-el-Banna¹ (Albanna) in the thirteenth century factored $10^n - 1$ for small values of n . The Arab Sibte el-Mâridini^{1a} in the fifteenth century noted that in the sexagesimal division of $47^\circ 50'$ by $1^\circ 25'$ the quotient has a period of eight terms.

G. W. Leibniz² in 1677 noted that $1/n$ gives rise to a purely periodic fraction to any base b , later adding the correction that n and b must be relatively prime. The length of the period of the decimal fraction for $1/n$, where n is prime to 10, is a divisor of $n - 1$ [erroneous for $n = 21$; cf. Wallis³].

John Wallis³ noted that, if N has a prime factor other than 2 and 5, the reduced fraction M/N equals an unending decimal fraction with a repetend of at most $N - 1$ digits. If N is not divisible by 2 or 5, the period has two digits if N divides 99, but not 9; three digits if N divides 999, but not 99. The period of $1/21$ has six digits and 6 is not a divisor of $21 - 1$. The length of the period for the reciprocal of a product equals the l. c. m. of the lengths of the periods of the reciprocals of the factors [cf. Bernoulli³]. Similar results hold for base 60 in place of 10.

J. H. Lambert⁴ noted that all periodic decimal fractions arise from rational fractions; if the period p has n digits and is preceded by a decimal with m digits, we have

$$a + \frac{b}{10^m} + r, \quad r = \frac{p}{10^m 10^n} + \frac{p}{10^m 10^{2n}} + \dots = \frac{p}{10^m (10^n - 1)}.$$

John Robertson⁵ noted that a pure periodic decimal with a period P of k digits equals $P/9 \dots 9$, where there are k digits 9.

J. H. Lambert⁶ concluded from Fermat's theorem that, if a is a prime other than 2 and 5, the number of terms in the period of $1/a$ is a divisor of $a - 1$. If g is odd and $1/g$ has a period of $g - 1$ terms, then g is a prime. If $1/g$ has a period of m terms, but $g - 1$ is not divisible by m , g is composite. Let $1/a$ have a period of $2m$ terms; if a is prime, $k = 10^m + 1$ is divisible by a ; if a is composite, k and a have a common factor; if k is divisible by a and if m is prime, each factor other than $2^p 5^q$ of a is of period $2m$.

Let a be a composite number not divisible by 2, 3 or 5. If $1/a$ has a period of m terms, where m is a prime, each factor of a produces a period

¹Cf. E. Lucas, *Arithmétique amusante*, 1895, 63-9; Brocard.¹⁰³

^{1a}Carra de Vaux, *Bibliotheca Math.*, (2), 13, 1899, 33-4.

²Manuscript in Bibliothek Hannover, vol. III, 24; XII, 2, Blatt 4; also, III, 25, Blatt 1, seq., 10, Jan., 1687. Cf. D. Mahnke, *Bibliotheca Math.*, (3), 13, 1912-3, 45-48.

³Treatise of Algebra both historical & practical, London, 1685, ch. 89, 326-8 (in manuscript, 1676).

⁴Acta Helvetica, 3, 1758, 128-132.

⁵Phil. Trans., London, 58, 1768, 207-213.

⁶Nova Acta Eruditorum, Lipsiæ, 1769, 107-128.

of m terms. If $1/a$ has a period of mn terms, where m and n are primes, while no factor has such a period, one factor of a divides $10^m - 1$ and another divides $10^n - 1$. If $1/a$ has a period of mnp terms, where m, n, p are primes, but no factor has such a period, any factor of a divides $10^m - 1, \dots$, or $10^{np} - 1$. These theorems aid in factoring a .

L. Euler⁷ gave numerical examples of the conversion of ordinary fractions into decimal fractions and the converse problem.

Euler^{7a} noted that if $2p+1$ is a prime $40n \pm 1, \pm 3, \pm 9, \pm 13$, it divides $10^p - 1$; if $2p+1$ is a prime $40n \pm 7, \pm 11, \pm 17, \pm 19$, it divides $10^p + 1$.

Jean Bernoulli⁸ gave a résumé of the work by Wallis,³ Robertson,⁵ Lambert⁶ and Euler,⁷ and gave a table showing the full period for $1/D$ for each odd prime $D < 200$, and a like table when D is a product of two equal or distinct primes < 25 . When the two primes are distinct, the table confirms Wallis' assertion that the length of the period for $1/D$ is the l. c. m. of the lengths of the periods for the reciprocals of the factors. But for $1/D^2$, where D is a prime > 3 , the length of the period equals D times that for $1/D$. If the period for $1/D$, where D is a prime, has $D-1$ digits, the period for m/D has the same digits permuted cyclically to begin with m . He gave (p. 310) a device communicated to him by Lambert: to find the period for $1/D$, where $D=181$, we find the remainder 7 after obtaining the part p composed of the first 15 digits of the period; multiply $1/D = p + 7/D$ by 7; thus the next 15 digits of the period are given by $7p$; since $7^3 = D + 162$, the third set of 15 digits is found by adding unity to 7^2p , etc.; since 7 belongs to the exponent 12 modulo D , the period for $1/D$ contains 15·12 digits.

Jean Bernoulli⁹ made use of various theorems due to Euler which give the possible linear forms of the divisors of $10^k \pm 1$, and obtained factors of $(10^k - 1)/9$ when $k \leq 30$, except for $k=11, 17, 19, 23, 29$, with doubt as to the primality of the largest factor when $k=13, 15$ or ≥ 19 . He stated (p. 325) erroneously¹⁰ that $(10^{11} + 1)/11 \cdot 23$ has no factor < 3000 . Also,

$$10^{15} + 1 = 7 \cdot 11 \cdot 13 \cdot 211 \cdot 9091 \cdot 52081.$$

He gave part of the periods for the reciprocals of various primes ≤ 601 .

L. Euler¹¹ wrote to Bernoulli concerning the latter's⁹ paper and stated criteria for the divisibility of $10^p \pm 1$ by a prime $2p+1 = 4n \pm 1$. If both 2 and 5 or neither occur among the divisors of n , $n \neq 2, n \neq 6$, then $10^p - 1$ is divisible by $2p+1$. But if only one of 2 and 5 occurs, then $10^p + 1$ is divisible by $2p+1$ [cf. Genocchi³⁹].

Henry Clarke¹² discussed the conversion of ordinary fractions into decimals without dealing with theoretical principles.

⁷Algebra, I, Ch. 12, 1770; French transl., 1774.

^{7a}Opusc. anal., 1, 1773, 242; Comm. Arith. Coll., 2, p. 10, p. 25.

⁸Nouv. mém. acad. roy. Berlin, année 1771 (1773), 273-317.

⁹Ibid., 318-337.

¹⁰P. Seelhoff, Zeitschrift Math. Phys., 31, 1886, 63. Reprinted, Sphinx-Oedipe, 5, 1910, 77-8.

¹¹Nouv. mém. acad. roy. Berlin, année 1772 (1774), Histoire, pp. 35-36; Comm. Arith., 1, 584.

¹²The rationale of circulating numbers, London, 1777, 1794.

Anton Felkel¹³ showed how to convert directly a periodic fraction written to one base into one to another base. He gave all primes < 1000 which can divide a period with a prime number of digits < 30 , as $29m+1 = 59, 233, \dots$

Oberreit¹⁴ extended Bernoulli's⁹ table of factors of $10^k \pm 1$.

C. F. Gauss¹⁵ gave a table showing the period of the decimal fraction for k/p^n , $p^n < 467$, p a prime, and the period for $1/p^n$, $467 \leq p^n \leq 997$.

W. F. Wucherer¹⁶ gave five places of the decimal fraction for n/d , $d < 1000$, $n < d$ for $d < 50$, $n \leq 10$ for $d \geq 50$.

Schröter published at Helmstadt in 1799 a table for converting ordinary fractions into decimal fractions.

C. F. Gauss¹⁷ proved that, if a is not divisible by the prime p ($p \neq 2, 5$), the length of the period for a/p^n is the exponent e to which 10 belongs modulo p^n . If we set $\phi(p^n) = ef$ and choose a primitive root r of p^n such that the index of 10 is f , we can easily deduce from the periods for k/p^n , where $k = 1, r, \dots, r^{f-1}$, the period for m/p^n , where m is any integer not divisible by p . For, if i be the index of m to the base r , and if $i = af + \beta$, where $0 \leq \beta < f$, we obtain the period for m/p^n from that for r^β/p^n by carrying the first a digits to the end. He computed¹⁵ the necessary periods for each $p^n < 1000$, but published here the table only to 100. By using partial fractions, we may employ the table to obtain the period for a/b , where b is a product of powers of primes within the limits of the table.

H. Goodwyn¹⁸ noted that, if $a < 17$, the period for $a/17$ is derived from the period for $1/17$ by a cyclic permutation of the digits. Thus we may print in a double line the periods for $1/17, \dots, 16/17$ by showing the period for $1/17$ and, above each digit d of the latter, showing the value of a such that the period for $a/17$ begins with the digit d , while the rest of the period is to be read cyclically from that for $1/17$.

Goodwyn¹⁹ noted that when $1/p$ is converted into a decimal fraction, p being prime, the sum of corresponding quotients in the two half periods is 9, and that for remainders is p , if $p \geq 7$.

J. C. Burckhardt²⁰ gave the length of the period for $1/p$ for each prime $p \leq 2543$ and for 22 higher primes. It follows that 10 is a primitive root of 148 of the 365 primes p , $5 < p < 2500$.

¹³Abhand. Böhmischen Gesell. Wiss., Prag, 1, 1785, 135-174.

¹⁴J. H. Lambert's Deutscher Gelehrter Briefwechsel, pub. by J. Bernoulli, Leipzig, vol. 5, 1787, 480-1. The part (464-479) relating to periodic decimals is mainly from Bernoulli's⁹ paper.

¹⁵Posthumous manuscript, dated Oct., 1795; Werke, 2, 1863, 412-434.

¹⁶Beyträge zum allgemeinem Gebrauch der Decimal Brüche. . . ., Carlsruhe, 1796.

¹⁷Disq. Arith., 1801, Arts. 312-8. A part was reproduced by Wertheim, Elemente der Zahlentheorie, 1887, 153-6.

¹⁸Jour. Nat. Phil. Chem. Arts (ed., Nicholson), London, 4, 1801, 402-3.

¹⁹Ibid., new series, 1, 1802, 314-6. Cf. R. Law, Ladies' Diary, 1824, 44-45, Quest. 1418.

²⁰Tables des diviseurs pour tous les nombres du premier million, Paris, 1817, p. 114. For errata see Shanks,⁶¹ Kessler,⁹² Cunningham,¹²⁴ and Gérardin.¹³¹

H. Goodwyn²¹ gave for each integer $d \leq 100$ a table of the periods for n/d , for the various integers $n < d$ and prime to d . Also, a table giving the first eight digits of the decimal equivalent to every irreducible vulgar fraction $< 1/2$, whose numerator and denominator are both ≤ 100 , arranged in order of magnitude, up to $1/2$.

Goodwyn^{22, 23} was without doubt the author of two tables, which refer to the preceding "short specimen" by the same author. The first gives the first eight digits of the decimal equivalent to every irreducible vulgar fraction, whose numerator and denominator are both ≤ 1000 , from $1/1000$ to $99/991$ arranged in order of magnitude. In the second volume, the "table of circles" occupies 107 pages and contains all the periods (circles) of every denominator prime to 10 up to 1024; there is added a two-page table showing the quotient of each number ≤ 1024 by its largest factor $2^a 5^b$.

For example, the entry in the "tabular series" under $\frac{57}{858}$ is .08689024. The entry in the two-page table under 656 is 41. Of the various entries under 41 in the "table of circles," the one containing the digits 9024 gives the complete period $\dot{9}024\dot{3}$. Hence $\frac{57}{858} = .08689024\dot{3}$.

Glaisher⁷⁸ gave a detailed account of Goodwyn's tables and checks on them. They are described in the British Assoc. Report, 1873, pp. 31-34, along with tables showing seven figures of the reciprocals of numbers < 100000 .

F. T. Poselger²⁴ considered the quotients $0, a, b, \dots$ and the remainders $1, \alpha, \beta, \dots$ obtained by dividing $1, A, A^2, \dots$ by the prime p ; thus

$$\frac{A}{p} = a + \frac{\alpha}{p}, \quad \frac{A^2}{p} = aA + b + \frac{\beta}{p}, \dots$$

Adding, we see that the sum $1 + \alpha + \beta + \dots$ of the remainders of the period is a multiple mp of p ; also, $m(A-1) = a + b + \dots$. Set

$$M = k + \dots + bA^{t-2} + aA^{t-1},$$

where A belongs to the exponent t modulo p . Then

$$\frac{A^{nt}}{p} = \frac{1}{p} + MS, \quad S = 1 + A^t + \dots + A^{(n-1)t}.$$

²¹The first centenary of a series of concise and useful tables of all the complete decimal quotients which can arise from dividing a unit, or any whole number less than each divisor, by all integers from 1 to 1024. To which is now added a tabular series of complete decimal quotients for all the proper vulgar fractions of which, when in their lowest terms, neither the numerator nor the denominator is greater than 100; with the equivalent vulgar fractions prefixed. By Henry Goodwyn, London, 1818, pp. xiv+18; vii+30. The first part was printed in 1816 for private circulation and cited by J. Farey in *Philos. Mag. and Journal*, London, 47, 1816, 385.

²²A tabular series of decimal quotients for all the proper vulgar fractions of which, when in their lowest terms, neither the numerator nor the denominator is greater than 1000, London, 1823, pp. v+153.

²³A table of the circles arising from the division of a unit, or any other whole number, by all the integers from 1 to 1024; being all the pure decimal quotients that can arise from this source, London, 1823, pp. v+118.

²⁴Abhand. Ak. Wiss. Berlin (Math.), 1827, 21-36.

If M is divisible by p , we may take $n=1$ and conclude that A'/p^2 differs from $1/p^2$ by an integer. If M is not divisible by p , S must be, so that n is divisible by p and the length of the period is pt . In general, for the denominator p^λ , we have $n=1$ if M is divisible by $p^{\lambda-1}$, but in the contrary case n is a multiple of $p^{\lambda-1}$. If the period for a prime p has an even number of digits, the sum of corresponding quotients in the two half periods is p .

An anonymous writer²⁵ noted that, if we add the digits of the period of a circulating decimal, then add the digits of the new sum, etc., we finally get 9. From a number subtract that obtained by reversing its digits; add the digits of the difference; repeat for the sum, etc.; we get 9.

Bredow²⁶ gave the periods for a/p , where p is a prime or power of a prime between 100 and 200. He gave certain factors of $10^n - 1$ for $n=6-10$, 12-16, 18, 21, 22, 28, 33, 35, 41, 44, 46, 58, 60, 96.

E. Midy²⁷ noted that, if a^n, a^{n_1}, \dots are the least powers of a which, diminished by unity, give remainders divisible by $q^h, q_1^{h_1}, \dots$, respectively (q, q_1, \dots being distinct primes), and if the quotients are not divisible by q, q_1, \dots , respectively, and if t is the l. c. m. of n, n_1, \dots , then a belongs to the exponent t modulo $p = q^h q_1^{h_1} \dots$, and $a^t - 1$ is divisible by q only h times.

Let the period of the pure decimal fraction for a/b have $2n$ digits. If b is prime to $10^n - 1$, the sum of corresponding digits in the half periods is always 9, and the sum of corresponding remainders is b . Next, let b and $10^n - 1$ have $d > 1$ as their g. c. d. and set $b' = b/d$. Let a_n be the n th remainder in finding the decimal fraction. Then $a + a_n = b'k$, $a_1 + a_{n+1} = b'k_1$, etc. The sums $q + q_n, q_1 + q_{n+1}, \dots$ of corresponding digits in the half periods equal

$$(10k - k_1)/d, \quad (10k_1 - k_2)/d, \dots, \quad (10k_{n-1} - k)/d.$$

Similar results hold when the period of mn digits is divided into n parts of m digits each. For example, in the period

0 0 2 4 8 1 3 8 9 5 7 8 1 6 3 7 7 1 7 1 2 1 5 8 8 0 8 9 3 3

for $1/403$, the two halves are not complementary ($10^{15} - 1$ being divisible by 31); for $i=1, 2, 3$, the sum of the digits of rank $i, i+3, i+6, \dots, i+27$ is always 45, while the corresponding sums of the remainders are 2015.

N. Druckenmüller^{27a} noted that any fraction can be expressed as $a/x + a_1/x^2 + \dots$.

J. Westerberg²⁸ gave in 1838 factors of $10^n \pm 1$ for $n \leq 15$.

G. R. Perkins²⁹ considered the remainder r_x when N^x is divided by P , and the quotient q in $Nr_{x-1} = Pq_x + r_x$. If $r_k = P - 1$, there are $2k$ terms in the period of remainders, and

$$r_{k+x} + r_x = P, \quad q_{k+x} + q_x = N - 1.$$

[These results relate to $1/P$ written to the base N .]

²⁵Polytechnisches Journal (ed., J. G. Dingler), Stuttgart, 34, 1829, 68; extract from *Mechanics' Magazine*, N. 313, p. 411.

²⁶Von den Perioden der Decimalbrüche, Progr., Oels, 1834.

²⁷De quelques propriétés des nombres et des fractions décimales périodiques, Nantes, 1836, 21 pp.

^{27a}Theorie der Kettenreihen. . . , Trier, 1837.

²⁸See Chapter on Perfect Numbers.¹⁰⁴

²⁹Amer. Jour. Sc. Arts, 40, 1841, 112-7.

E. Catalan³⁰ converted periodic decimals into ordinary fractions without using infinite progressions. When $1/13$ is converted into a decimal, the period of remainders is 1, 10, 9, 12, 3, 4; repeat the period; starting in the series of 12 terms with any term (as 10), take the fourth term (4) after it, the fourth term (12) after that, etc.; then the sum 26 of the three is a multiple of 13. In general, if D is a prime and $D-1=mn$, the sum of n terms taken m by m in the period for N/D is a multiple of D [cf. Thibault³¹].

If the sum of two terms of the period of remainders for N/D is D , the same is true of the terms following them. Hence the sum of corresponding terms of the two half periods is D . This happens if the number of terms of the period is $\phi(D)$.

Thibault³¹ denoted the numbers of digits in the periods for $1/d$ and $1/d'$ by m and m' . If d' is divisible by d , m' is divisible by m . If d and d' have no common prime factor other than 2 or 5, the number of digits in the period for $1/dd'$ is the l. c. m. of m, m' . Hence it suffices to know the length of the period for $1/p^a$, where p is a prime. If $1/p$ has a period of m digits and if $1/p^n$ is the last one of the series $1/p, 1/p^2, \dots$ which has a period of m digits, then the period for $1/p^a$ for $a > n$ has mp^{a-n} digits. For $p=3$, we have $n=2$; hence $1/3^r$ for $r \geq 2$ has a period of 3^{r-2} digits. For any prime p for which $7 \leq p \leq 101$, we have $n=1$, so that $1/p^a$ has a period of mp^{a-1} digits. Note that $1/p$ and $1/p^2$ have periods of the same length to base b if and only if $b^{p-1} \equiv 1 \pmod{p^2}$. Proof is given of Catalan's³⁰ first theorem, which holds only when $10^m \not\equiv 1 \pmod{D}$, i. e., when m is not a multiple of the number of digits in the period. For example, the sum of the k th and $(6+k)$ th remainders for $1/13$ is not a multiple of 13.

E. Prouhet³² proved Thibault's³¹ theorem on the period for $1/p^n$. He^{32a} noted that multiples of 142857 have the same digits permuted.

P. Lafitte³³ proved Midy's²⁷ theorem that, if p is a prime not dividing m and if the period for m/p has an even number of digits, the sum of the two halves of the period is $9 \dots 9$.

J. Sornin³⁴ investigated the number m of digits in the period for $1/D$, where D is prime to 10. The period is $x = (10^m - 1)/D$. First, let $D = 10k + 1$. Then $x = 10y - 1$, where

$$y = \frac{10^{m-1} + k}{D} = 10z + k, \quad z = \frac{10^{m-2} - k^2}{D}.$$

Finally, we reach $v = \{1 - (-k)^m\}/D$, and x is an integer if and only if v is. Hence if we form the powers of the number k of tens in D , add 1 to the odd powers, but subtract 1 from the even powers of k , the first exponent giving a result divisible by D is the number m of digits in the period.

³⁰Nouv. Ann. Math., 1, 1842, 464-5, 467-9.

³¹*Ibid.*, 2, 1843, 80-89.

³²*Ibid.*, 5, 1846, 661.

^{32a}*Ibid.*, 3, 1844, 376; 1851, 147-152.

³³*Ibid.*, 397-9. Cf. Amer. Math. Monthly, 19, 1912, 130-2.

³⁴*Ibid.*, 8, 1849, 50-57.

Next, if $D = 10k - 1$, we have a like rule to be applied only to the $k^m - 1$. If $D = 10k \pm 3$, $1/(3D)$ has a denominator $10l \neq 1$, and the length of its period, found as above, is shown to be not less than that for $1/D$.

Th. Bertram³⁵ gave certain numbers p for which $1/p$ has a given length k of period for $k \leq 100$. Cf. Shanks.⁶²

J. R. Young³⁶ took a part of a periodic decimal, as .1428571 428 for $1/7$, and marked off from the end a certain number (three) of digits. We can find a multiplier (as 6) such that the product, with the proper carrying (here 2) from the part marked off, has all the digits of the abridged number in the same cyclic order, except certain of the leading digits. In the special case the product is .8571428.

W. Loof³⁷ gave the primes p for which the period for $1/p$ has a given number n of digits, $n \leq 60$, with no entry for $n = 17, 19, 37-40, 47, 49, 57, 59$, and with doubt as to the primality of large numbers entered for various other n 's.

E. Desmarest³⁸ gave the primes $P < 10000$ for which 10 belongs to the exponent $(P-1)/t$ for successive values of t . The table thus gives the length of the period for $1/P$. He stated (pp. 294-5) that if P is a prime < 1000 , and if p is the length of the period for A/P , then except for $P = 3$ and $P = 487$ the length of the period for A/P^2 is pP .

A. Genocchi³⁹ proved Euler's¹¹ rule by use of the quadratic reciprocity law. Thus 5 is a quadratic residue or non-residue of N according as $N = 5m \pm 1$ or $5m \pm 3$; for $4n + 1 = 5m \pm 1$, n or $n - 2$ is divisible by 5; for $4n - 1 = 5m \pm 1$, n or $n + 2$ is divisible by 5. Also, 2 is a residue of $4n \pm 1$ for n even, a non-residue for n odd. Hence 10 is a residue of $N = 4n \pm 1$ for n even if n or $n \mp 2$ is divisible by 5, and for n odd if neither is. Thus Euler's inclusion of $n \mp 6$ is superfluous. By a similar proof, 10 is quadratic non-residue of $N = 4n \pm 1$ if both 2 and 5 occur among the divisors of $n \mp 2$, $n \mp 6$, or if neither occurs; a residue if a single one of them occurs.

A. P. Reyer^{39a} noted that the period for $a/3^p$ has 3^{p-2} digits and gave the length of the period for a/p for each prime $p < 150$.

*F. van Henekeler^{39b} treated decimal fractions.

C. G. Reuschle⁴⁰ gave for each prime $p < 15000$ the exponent e to which 10 belongs modulo p . Thus e is the length of the period for $1/p$. He gave all the prime factors of $10^n - 1$ for $n \leq 16$, $n = 18, 20, 21, 22, 24, 26, 28, 30, 32, 36, 42$; those of $10^n + 1$ for $n \leq 18$, $n = 21$; also cases up to $n = 243$ of the factors of the quotient obtained by excluding analytic factors.

³⁵Einige Sätze aus der Zahlenlehre, Progr. Cöln, Berlin, 1849, 14-15.

³⁶London, Ed. Dublin Phil. Mag., 36, 1850, 15-20.

³⁷Archiv Math. Phys., 16, 1851, 54-57. French transl. in Nouv. Ann. Math., 14, 1855, 115-7. Quoted by Brocard, Mathesis, 4, 1884, 38.

³⁸Théorie des nombres, Paris, 1852, 308. For errata, see Shanks⁶¹ and Gérardin.¹³¹

³⁹Bull. Acad. Roy. Sc. Belgique, 20, II, 1853, 397-400.

^{39a}Archiv Math. Phys., 25, 1855, 190-6.

^{39b}Ueber die primitiven Wurzeln der Zahlen und ihre Anwendung auf Dezimalbrüche, Leyden, 1855 (Dutch).

⁴⁰Math. Abhandlung... Tabellen, Progr. Stuttgart, 1856. Full title in Ch. I.¹⁰⁸ Errata, Bork,¹⁰⁵ Hertzner,¹¹⁹ Cunningham.¹²¹

W. Stammer⁴¹ noted that $n/p = 0.\dot{a}_1 \dots \dot{a}_x$ implies

$$\frac{n}{p}(10^x - 1) = a_1 \dots a_x.$$

J. B. Sturm⁴² used this result to explain the conversion of decimal into ordinary fractions without the use of series.

M. Collins⁴³ stated that, if we multiply any decimal fraction having m digits in its period by one with n digits, we obtain a product with $9mn$ digits in its period if m is prime to n , but with $n(10^m - 1)$ digits if n is divisible by m .

J. E. Oliver⁴⁴ proved the last theorem. If x'/x gives a periodic fraction to the base a with a period of ξ figures, then $a^\xi \equiv 1 \pmod{x}$ and conversely. The product of the periodic fractions for $x'/x, \dots, z'/z$ with period lengths ξ, \dots, ζ has the period length

$$\frac{x \dots z}{M(x, \dots, z)} \cdot M(\xi, \dots, \zeta),$$

where $M(x, \dots, z)$ is the l. c. m. of x, \dots, z . He examined the cases in which the first factor in the formula is expressible in terms of ξ, \dots, ζ .

Fr. Heime⁴⁵ and M. Pokorny⁴⁶ gave expositions without novelty.

Suffield⁴⁷ gave the more important rules for periodic decimals and indicated the close connection with the method of synthetic division.

W. H. H. Hudson⁴⁸ called d a proper prime if the period for n/d has $d - 1$ digits. If the period for r/p has $n = (p - 1)/\lambda$ digits, there are λ periods for p . The sum of the digits in the period for a proper prime p is $9(p - 1)/2$. If $1/p$ has a period of $2n$ digits, the sum of corresponding digits in the two half periods is 9, and this holds also if p is composite but has no factor dividing $10^n - 1$ [Midy²⁷]. If $10p + 1$ is a proper prime, each digit $0, 1, \dots, 9$ occurs p times in its period. If a, b are distinct primes with periods of α, β digits, the number of digits in the period for ab is the l. c. m. of α, β [Bernoulli⁸]. Let p have a period of n digits and $1/p = k/(10^n - 1)$. Let m be the least integer for which

$$\binom{m}{1} \frac{k}{p^{x-1}} + \binom{m}{2} \frac{k^2}{p^{x-2}} + \dots + \binom{m}{x-1} \frac{k^{x-1}}{p}$$

is an integer; then $1/p^x$ has a period of mn digits.

⁴¹Archiv Math. Phys., 27, 1856, 124.

⁴²*Ibid.*, 33, 1859, 94-95.

⁴³Math. Monthly (ed., Runkle), Cambridge, Mass., 1, 1859, 295.

⁴⁴*Ibid.*, 345-9.

⁴⁵Ueber relative Prim- und correspondirende Zahlen, primitive und sekundäre Wurzeln und periodische Decimalbrüche, Progr., Berlin, 1860, 18 pp.

⁴⁶Ueber einige Eigenschaften periodischer Dezimalbrüche, Prag, 1864.

⁴⁷Synthetic division in arithmetic, with some introductory remarks on the period of circulating decimals, 1863, pp. iv + 19.

⁴⁸Oxford, Cambridge and Dublin Messenger of Math., 2, 1864, 1-6. Glaisher⁷⁸ attributed this useful anonymous paper to Hudson.

V. A. Lebesgue⁴⁹ gave for $N \leq 347$ the periods for $1/N, r/N, \dots$ [cf. Gauss¹⁷].

Sanio⁵⁰ stated that, if m, n, \dots are distinct primes and $1/m, 1/n, \dots$ have periods of length q, q', \dots , then $1/(m^a n^b \dots)$ has the period length $m^{a-1} n^{b-1} \dots qq' \dots$. He gave the length of the period for $1/p$ for each prime $p \leq 700$, and the factors of $10^n - 1, n \leq 18$.

F. J. E. Lionnet⁵¹ stated that, if the period for a/b has n digits, that for any irreducible fraction whose denominator is a multiple of b has a multiple of n digits. If the periods for the irreducible fractions $a/b, a'/b', \dots$ have n, n', \dots digits, every irreducible fraction whose denominator is the l. c. m. of b, b', \dots has a period whose length is the l. c. m. of n, n', \dots . If the period for $1/p$ has n digits and if p^a is the highest power of the prime p which divides $10^n - 1$, any irreducible fraction with the denominator $p^{a+\beta}$ has a period of np^β digits.

C. A. Laisant and E. Beaujeux⁵² proved that if q is a prime and the period for $1/q$ to the base B is $P = ab \dots h$, with $q-1$ digits, then

$$P - (a + b + \dots + h) = (B-1)\sigma, \quad q \left(\sigma + \frac{q-1}{2} \right) = \frac{B^{q-1} - 1}{B-1},$$

and stated that a like result holds for a composite number q if we replace $q-1$ by $f = \phi(q)$. Their proof of the generalized Fermat theorem $B^f \equiv 1 \pmod{q}$ is quoted under that topic.

C. Sardi⁵³ noted that if 10 is a primitive root of a prime $p = 10n + 1$, the period for $1/p$ contains each digit $0, \dots, 9$ exactly n times [Hudson⁴⁸]. For $p = 10n + 3$, this is true of the digits other than 3 and 6, which occur $n+1$ times. Analogous results are given for $10n + 7, 10n + 9$.

Ferdinand Meyer⁵⁴ proved an immediate generalization from 10 to any base k prime to b, b', \dots of the statements by Lionnet.⁵¹

Lehmann^{54a} gave a clear exposition of the theory.

C. A. Laisant and E. Beaujeux⁵⁵ considered the residues r_0, r_1, \dots when A, AB, AB^2, \dots are divided by D_1 . Let $r_{i-1}B = Q_i D_1 + r_i$. When written to the base B , let $D_1 = a_p \dots a_2 a_1$, and set $D_i = a_p \dots a_i$. Then

$$a_1 r_1 + \dots + a_p r_p = D_1 (r_1 - Q_2 D_2 - \dots - Q_p D_p).$$

The further results are either evident or not novel.

For G. Barillari^{60a} on the length of the period, see Ch. VII.

⁴⁹Mém. soc. sc. phys. et nat. de Bordeaux, 3, 1864, 245.

⁵⁰Ueber die periodischen Decimalbrüche, Progr., Memel, 1866.

⁵¹Algèbre élém., ed. 3, 1868. Nouv. Ann. Math., (2), 7, 1868, 239. Proofs by Morel and Pellet, (2), 10, 1871, 39-42, 92-95.

⁵²Nouv. Ann. Math., (2), 7, 1868, 289-304.

⁵³Giornale di Mat., 7, 1869, 24-27.

⁵⁴Archiv Math. Phys., 49, 1869, 168-178.

^{54a}Ueber Dezimalbrüche, welche aus gewöhnlichen Brüchen abgeleitet sind, Progr., Leipzig, 1869.

⁵⁵Nouv. Ann. Math., (2), 9, 1870, 221-9, 271-281, 302-7, 354-360.

*Th. Schröder⁵⁶ and J. Hartmann⁵⁷ treated periodic decimals.

W. Shanks⁵⁸ gave Lambert's method (Bernoulli,⁸ end) for shortening the work of finding the length of the period for $1/N$.

G. Salmon⁵⁹ remarked that the number n of digits in the period is known if we find two remainders which are powers of 2, since $10^a \equiv 2^p$ and $10^b \equiv 2^q$ imply $10^{aq-bp} \equiv 1$; also if we find three remainders which are products of powers of 2 and 3. Muir⁷¹ noted that it is here implied that $aq-bp$ equals n , whereas it is merely a multiple of n .

J. W. L. Glaisher⁶⁰ proved that, for any base r ,

$$\frac{1}{(r-1)^2} = .012 \dots \overline{r-3} \overline{r-1},$$

a generalization of $1/81 = .\dot{0}12345679$.

W. Shanks⁶¹ gave the length of the period for $1/p$, when p is a prime < 30000 , and a list of 69 errors or misprints in the table by Desmarest,³⁸ and 11 in that by Burckhardt.²⁰

Shanks⁶² gave primes p for which the length n of the period for $1/p$ is a given number ≤ 100 , naturally incomplete. Shanks⁶³ gave additional entries p for $n=26$, $n=99$; noted corrections to his former table and stated that he had extended the table to 40000. Shanks⁶⁴ mentioned an extension in manuscript from 40000 to 60000. An extension to 120000 in manuscript was made by Shanks, 1875-1880. The manuscript, described by Cunningham,¹²⁴ who gave a list of errata, is in the Archives of the Royal Society of London.

Shanks⁶⁵ stated that if a is the length of the period for $1/p$, where p is a prime > 5 , that for $1/p^n$ is ap^{n-1} [without the restriction by Thibault,³¹ Muir⁷¹].

G. de Coninck⁶⁶ stated that, if the last digit (at the right) of A is 1 or 9, the last digit of the period for $1/A$ is 9 or 1; while, if A is a prime not ending in 1 or 9, its last digit is the same as the last in the period.

Moret-Blanc⁶⁷ noted that the last property holds for any A not divisible by 2 or 5. For, if a is the integer defined by the period for $1/A$, that for $(A-1)/A$ is $(A-1)a$, whence $a + (A-1)a = 10^n - 1$, if n is the length of the periods. He noted corrections to the remaining nine laws stated by Coninck and implied that when corrected they become trivial or else known facts.

⁵⁶Progr. Ansbach, 1872.

⁵⁷Progr. Rinteln, 1872.

⁵⁸Messenger Math., 2, 1873, 41-43.

⁵⁹Ibid., pp. 49-51, 80.

⁶⁰Ibid., p. 188.

⁶¹Proc. Roy. Soc. London, 22, 1873-4, 200-10, 384-8. Corrections by Workman.¹¹⁷

⁶²Ibid., pp. 381-4. Cf. Bertram¹⁴, Loof.³⁷

⁶³Ibid., 23, 1874-5, 260-1.

⁶⁴Ibid., 24, 1875-6, 392.

⁶⁵Messenger Math., 3, 1874, 52-55.

⁶⁶Nouv. Ann. Math., (2), 13, 1874, 569-71; errata, 14, 1875, 191-2.

⁶⁷Ibid., (2), 14, 1875, 229-231.

Karl Broda⁶⁸ considered a periodic decimal fraction F having an even number r of digits in the period and a number m of p digits preceding the period. Let x be the first half of the period, y the second half. Then

$$F = \frac{p}{10^m} + \frac{x}{10^{m+r}} + \frac{y}{10^{m+2r}} + \frac{x}{10^{m+3r}} + \dots = \frac{p}{10^m} + \frac{10^r x + y}{10^m(10^{2r}-1)} \\ = \frac{9(p \cdot 10^r + x + p) + a}{9 \cdot 10^m(10^r + 1)}$$

if $x+y=a(10^r-1)/9=a\dots a$ (to r terms). The first paper treated the case $p=m=0$, and gave the generalization to base a in place of 10:

$$\frac{x}{a^r} + \frac{y}{a^{2r}} + \frac{x}{a^{3r}} + \dots = \frac{a+(a-1)x}{(a-1)(a^r+1)} \quad \text{if } x+y=a \frac{a^r-1}{a-1}.$$

The case $a=a-1$ shows that a purely periodic fraction to the base a equals $(x+1)/(a^r+1)$ if the sum of the half periods has all its digits (to base a) equal to $a-1$. Returning to the base 10, and taking $N=9(10^r+1)$, $Z=9x+a$, where each digit of x is $\leq a$, we see that Z/N equals a decimal fraction in which x is the first half of the period of r digits, while the second half is such that the sum of corresponding digits in it and x is a . If R is the remainder after r digits of the period have been obtained, $R+Z=a(10^r+1)$.

C. G. Reuschle⁶⁹ gave tables which serve to find numbers belonging to a given exponent < 100 with respect to a given prime modulus < 1000 .

P. Mansion⁷⁰ gave a detailed proof that, if n is prime to 2, 3, 5, and if the period for $1/n$ has $n-1$ digits, the sum of corresponding digits in the half periods is 9.

T. Muir⁷¹ proved that, if p is a prime, either of

$$N^x \equiv 1 \pmod{p^s}, \quad N^{xp^n} \equiv 1 \pmod{p^{s+n}}$$

follows from the other. If x_1 is the least positive integer x for which the first holds and if p^s is the highest power of p dividing $N^{x_1}-1$, then $x_1 p^n$ is the least positive integer y for which $N^y \equiv 1 \pmod{p^{s+n}}$. Hence the known theorem: If $N = \prod p_i^{n_i}$, where p_1, p_2, \dots are distinct primes, and if the period for $1/p_i$ has m_i digits, and if $p_i^{b_i}$ is the highest power of p_i dividing $10^{m_i}-1$, the number of digits in the period for $1/N$ is the l. c. m. of the $m_i p_i^{n_i-b_i}$. He asked if $b=1$ when $p>3$, as affirmed by Shanks.⁶⁵

Mansion's proof (*ibid.*, 5, 1876, 33) by use of periodic decimals of the generalized Fermat theorem is quoted under that topic.

D. M. Sensenig⁷² noted that a prime $p \neq 2, 5$, divides N if it divides the sum of the digits of N taken in sets of as many figures each as there are digits in the period for $1/p$.

⁶⁸Archiv Math. Phys., 56, 1874, 85-98; 57, 1875, 297-301.

⁶⁹Tafeln complexer Primzahlen, Berlin, 1875. Errata by Cunningham, Mess. Math., 46, 1916, 60-1.

⁷⁰Nouv. Corresp. Math., 1, 1874-5, 8-12.

⁷¹Messenger Math., 4, 1875, 1-5.

⁷²The Analyst, Des Moines, Iowa, 3, 1876, 25.

*A. J. M. Brogtrop⁷³ treated periodic decimals.

G. Bellavitis⁷⁴ noted that the use of base 2 renders much more compact and convenient Gauss'¹⁵ table and hence constructed such a table.

W. Shanks⁷⁵ found that the period for $1/p$, where $p=487$, is divisible by p , so that the period for $1/p^2$ has $p-1$ digits.

J. W. L. Glaisher⁷⁶ formed the period 05263... for $1/19$ as follows: List 5; divide it by 2 and list the quotient 2; since the remainder is 1, divide 12 by 2 and list the quotient 6; divide it by 2 and list the quotient, etc. To get the period for $1/199$, start with 50. To get the period, apart from the prefixed zero, for $1/49$, start with 20 and divide always by 5; for $1/499$, start with 200.

Glaisher⁷⁷ noted that, if we regard as the same periods those in which the digits and their cyclic order are the same, even if commencing at different places, a number q prime to 10 will have f periods each of a digits, where $af=\phi(q)$. This was used to check Goodwyn's table.²³ If $q=39$, there are four periods each of six digits. If $q-1$ belongs to the period for $1/q$, the two halves of every period are complementary; if not, the periods form pairs and the periods in each pair are complementary. For each prime $N<1000$, except 3 and 487, the period for $1/N^k$ has nN^{k-1} digits if that for $1/N$ has n digits.

Glaisher⁷⁸ collected various known results on periodic decimals and gave an account of the tables relating thereto. If q is prime to 10 and if the period for $1/q$ has $\phi(q)$ digits, the products of the period by the $\phi(q)$ integers $<q$ and prime to q have the same digits in the same cyclic order; for example, if $q=49$. He gave (pp. 204-6) for each $q<1024$ and prime to 10 the number a of digits in the period for $1/q$, the number n of periods of irreducible fractions p/q , not regarding as distinct two periods having the same digits in the same cyclic order, and, finally Euler's $\phi(q)$. The values of a and n were obtained by mere counting from the entries in Goodwyn's²³ "table of circles"; in every case, $an=\phi(q)$. For the prime $p=487$, he gave the full periods for $1/p$ and $1/p^2$, each of 486 digits, thus verifying Desmarest's³⁸ statement of the exceptional character of this p [cf. Shanks⁷⁵].

Glaisher⁷⁹ again stated the chief rules for the lengths of periods.

The problem was proposed⁸⁰ to find a number whose products by 2, ..., 6 have the same digits, but in a new order.

Birger Hausted⁸¹ solved this problem. Start with any number a of one digit, multiply it by any number p and let b be the digit in the units

⁷³Nieuw Archief voor Wiskunde, Amsterdam, 3, 1877, 58-9.

⁷⁴Atti Accad. Lincei, Mem. Sc. Fis. Mat., (3), 1, 1877, 778-800. Transunti, 206. See 62a of Ch. VII.

⁷⁵Proc. Roy. Soc. London, 25, 1877, 551-3.

⁷⁶Messenger Math., 7, 1878, 190-1. Cf. Desmarest.³⁸

⁷⁷Report British Assoc., 1878, 471-3.

⁷⁸Proc. Cambridge Phil. Soc., 3, 1878, 185-206.

⁷⁹Solutions of the Cambridge Senate-House Problems and Riders for 1878, pp. 8-9.

⁸⁰Tidsskrift for Math., Kjobenhavn, 2, 1878, 28.

⁸¹Ibid., pp. 180-3. Jornal de Sc. Math. e Ast., 2, 1878, 154-6.

place of the product ap , β the digit in the tens place. Write the digit b to the left of digit a to form the last two digits of the required number P . The number c in the units place in $bp + \beta$ is written to the left of digit b in P . To cp add the digit in the tens place of bp and place the unit digit of the sum to the left of c in P . The process stops with the k th digit t if the next digit would give a . Then $P = t \dots cba$ and its products by k integers or fractions has the same k digits in the same cyclic order. For $a=2$, $p=3$, we get $k=28$ and see that P is the period of $2/27$, and the k multipliers are $m/2$, $m=1, \dots, 28$. [To have an example simpler than the author's, take $a=7$, $p=5$; then $P=142857$, the period of $1/7$; the multipliers are $1, \dots, 6$.] For proof, we have

$$P = 10^{k-1}t + \dots + 10^2c + 10b + a, \quad pP = 10^{k-1}a + 10^{k-2}t + \dots + 10c + b,$$

$$pP = 10^{k-1}a + \frac{P-a}{10}, \quad \frac{a}{10p-1} = \frac{P}{10^k-1},$$

so that P is the period with k digits for $a/(10p-1)$.

E. Lucas⁸² gave the prime factors of $10^{13} \pm 1$, $10^{17} \pm 1$, $10^{21} \pm 1$, $10^{16} + 1$, $10^{18} + 1$, communicated to him by W. Loof, with the remark that $(10^{19} - 1)/9$ has no prime factor < 3035479 . Lucas gave the factors of $10^{30} + 1$.

J. W. L. Glaisher⁸³ proved his⁷⁶ earlier statements, repeated his⁷⁷ earlier remarks, and noted that, if q is a prime such that the period for $1/q$ has $q-1$ digits, the products of the period for $1/q$ by $1, 2, \dots, q-1$ have the same digits in the same cyclic order. This property, well known for $q=7$, holds also for $q=17, 19, 23, 29, 47, 59, 61, 97$ and for $q=7^2$.

O. Schlömilch⁸⁴ stated that, to find every N for which the period for $1/N$ has $2k$ digits such that the sum of the s th and $(k+s)$ th digits is 9 for $s=1, \dots, k$, we must take an integer $N = (10^k + 1)/T$; then the first k digits of the period are the k digits of $T-1$.

C. A. Laisant⁸⁵ extended his investigations with Beaujeux^{52,55} and gave a summary of known properties of periodic fractions; also his⁸⁶ process to find the period of simple periodic fractions without making divisions.

V. Bouniakowsky⁸⁷ noted that the property of the period of $1/N$, observed by Schlömilch⁸⁴ for $N=7, 11, 13, 77, 91, 143$, holds also for the periods of k/N , for $k=N-1$ and $(N-1)/2$, with the same values of N . Consider the decimal fraction $0.y_1y_2\dots$ with $y_m \equiv y_{m-1} + y_{m-2} \pmod{9}$, replacing any residue zero by 9, and taking $y_1 > 0$, $y_2 > 0$. The fraction is purely periodic and is either $0.\dot{9}$ or $0.\dot{3}369663\dot{9}$ or has the same digits permuted cyclically, or else has a period of 24 digits and begins with 1, 1 or 2, 2 or 4, 4, or has the same 24 digits permuted cyclically or by the interchange of the two halves

⁸²Nouv. Corresp. Math., 5, 1879, 138-9.

⁸³Nature, 19, 1879, 208-9.

⁸⁴Zeitschrift Math. Phys., 25, 1880, 416.

⁸⁵Mém. Soc. Sc. Phys. et Nat. de Bordeaux, (2), 3, 1880, 213-34.

⁸⁶Les Mondes, 19, 1869, 331.

⁸⁷Bull. Acad. Sc. St. Pétersbourg, 27, 1881, 362-9.

of the period. The property of Schlömilch holds for these and the generalization to any base, as well as for those with the law $y_m \equiv 2y_{m-1} + y_{m-2}$. But if $y_m \equiv 3y_{m-1} - 2y_{m-2} \pmod{9}$, $y_m \equiv (2^{m-1} - 1)(y_2 - y_1) + y_1 \pmod{9}$, the fact that $2^6 \equiv 1 \pmod{9}$ shows that the period has at most six digits. Those with six reduce by cyclic permutation to nine periods:

167943, 235986, 278154, 197346,
265389, 218457, 764913, 329568, 751248.

In the k th of these the sum of corresponding digits in the two half periods is always $\equiv k \pmod{9}$.

Karl Broda⁸⁸ examined for small values of r and certain primes p the solutions x of $x^r \equiv 1 \pmod{p}$ to obtain a base x for which the periodic fraction for $1/p$ has a period of r digits, and similarly the condition $x^r \equiv -1 \pmod{p}$ for an even number of digits in the period (Broda⁶⁸).

F. Kessler⁸⁹ factored $10^n - 1$ for $n = 11, 20, 22, 30$.

W. W. Johnson⁹⁰ formed the period for $1/19$ by placing 1 at the extreme right, next its double, etc., marking with a star a digit when there is 1 to carry:

* * * * * * * *
0 5 2 6 3 1 5 7 8 9 4 7 3 6 8 4 2 1.

To deduce the value of $1/19$ written to the base 2, use 1 for each digit starred and 0 for the others, reversing the order:

.0 0 0 0 1 1 0 1 0 1 1 1 1 0 0 1 0 1.

If we apply the first process with the multiplier m , we get the period for the reciprocal of $10m - 1$.

E. Lucas⁹¹ gave the prime factors of $10^n - 1$ for n odd, $n \leq 17$, $n = 21$, and certain factors for $n = 19, \dots, 41$; those of $10^n + 1$ for $n \leq 18$ and $n = 21$. He stated that the majority of the results were given by Loof and published by Reuschle. In 1886, Le Lasseur gave

$$10^{17} - 1 = 3^2 \cdot 2071723 \cdot 5363222[3]57,$$

said by Loof to have no divisor $< 400,000$ other than 3, 9. On the omission of the digit 3, see Cunningham.¹²³

F. Kessler⁹² listed nine errors in Burckhardt's²⁰ table and described his own manuscript of a table to $p = 12553$, i. e., for the first 1500 primes.

Van den Broeck⁹³ stated that $10^{3^n} - 1$ is divisible by 3^{n+2} .

A. Lugli⁹⁴ proved that, if p is a prime $\neq 2, 5$, the length of the period of $1/p$ is a divisor of $p - 1$. If the number of digits in the period of a/p is an even number $2t$, the t th remainder on dividing a by p is $p - 1$, and conversely. Hence, if r_h is the h th remainder, $r_h + r_{h+t} = p$ ($h = 1, \dots, t$), and the sum of all the r 's is tp . If the period of $1/p$ has s digits, $s < p - 1$, then

⁸⁸Archiv Math. Phys., 68, 1882, 85-99.

⁸⁹Zeitschrift Math. Naturw. Unterricht, 15, 1884, 29.

⁹⁰Messenger of Math., 14, 1884-5, 14-18.

⁹¹Jour. de math. élém., (2), 10, 1886, 160. Cf. l'intermédiaire des math., 10, 1903, 183. Quoted by Brocard, Mathesis, 6, 1886, 153; 7, 1887, 73 (correction, 1889, 110).

⁹²Archiv Math. Phys., (2), 3, 1886, 99-102.

⁹³Mathesis, 6, 1886, 70. Proofs, 235-6, and Math. Quest. Educ. Times, 54, 1891, 117.

⁹⁴Periodico di Mat., 2, 1887, 161-174.

$p-1=sh$ and we have h sets of s fractions whose periods differ only by the cyclic permutation of the digits. If p is a product of distinct primes p_1, p_2, \dots and if the lengths of the periods of $1/p, 1/p_1, 1/p_2, \dots$ are s, s_1, s_2, \dots , then s is the l. c. m. of s_1, s_2, \dots . If $p=p_1^a p_2^b \dots$, and s, s_1, s' are the lengths of the periods of $1/p, 1/p_1, 1/p_1^a$, then s' is one of the numbers $s_1, s_1 p, \dots, s_1 p_1^{a-1}$ and hence divides $(p_1-1)p_1^{a-1}$; and s is a divisor of $\phi(p)$. Thus p divides $10^{\phi(p)}-1$.

C. A. Laisant⁹⁵ used a lattice of points, whose abscissas are $a+r, a+2r, \dots, a+pr$ and ordinates are their residues $< p$ modulo p , to represent graphically periodic decimal fractions and to expand fractions into a difference of two series of ascending powers of fixed fractions.

*A. Rieke⁹⁶ noted that a periodic decimal with a period of $2m$ digits equals $(A+1)/(10^m+1)$, where A is the first half of the period. He discussed the period length for any base.

W. E. Heal⁹⁷ noted that, if B contains all the prime factors of N , the number of digits in the fraction to the base B for M/N is the greatest integer in $(n+n'-1)/n'$, where $n-n'$ is the greatest difference found by subtracting the exponent of each prime factor of N from the exponent of the same prime factor of B . If B contains no prime factor of N , the fraction for M/N is purely periodic, with a period of $\phi(N)$ digits. If B contains some, but not all, of the prime factors of N , the number of digits preceding the period is the same as in the first theorem. The proofs are obscure. There is given the period for $1/p$ when $p < 100$ and has 10 as a primitive root [the same p 's as by Glaisher⁸³]. Likewise for base 12, with $p < 50$.

R. W. Genese⁹⁸ noted that, if we multiply the period for $1/81$ [Glaisher⁶⁰] by m , where $m < 81$ and prime to it, we get a period containing the digits 0, 1, \dots , 9 except $9n-m$, where $9n$ is the multiple of 9 just exceeding m .

Jos. Mayer⁹⁹ investigated the moduli with respect to which 10 belongs to a given exponent, and gave the factors of 10^n-1 , $n < 12$. He discussed the determination of the exponent to which 10 belongs for a given modulus by use of the theory of indices and by the methods of quadratic, cubic, biquadratic, \dots residues. He used also the fact that there are $(a-a')(\beta-\beta') \dots$ divisors of $p_1^a p_2^b p_3^c \dots$ which divide no one of the fixed factors $p_1^a p_2^b p_3^c \dots, p_1^a p_2^b p_3^c \dots$, where $a < a', b < \beta, \dots$, and p_1, p_2, \dots are distinct primes. He gave the length of the period for $1/p$, for each prime $p \leq 2543$ and 22 higher primes [Burckhardt²⁰].

L. Contejean¹⁰⁰ proved that, in the conversion of an irreducible fraction a/b into a decimal fraction, if the remainders a_r and a_m are congruent modulo b , so that $10^r a \equiv 10^m a$, then $10^{m-r}-1$ is divisible by the quotient b' of b by the highest factor $2^s 5^t$ of b . Thus the length of the period is

⁹⁵Assoc. franç. avanc. sc., 16, 1887, II, 228-235.

⁹⁶Versuch über die periodischen Brüche, Progr., Riga, 1887.

⁹⁷Annals of Math., 3, 1887, 97-103.

⁹⁸Report British Assoc., 1888, 580-1.

⁹⁹Ueber die Grösse der Periode eines unendlichen Dezimalbruches, oder die Congruence $10^x \equiv 1 \pmod{P}$. Progr. K. Studienanstalt Burghausen, München, 1888, 52 pp.

¹⁰⁰Bull. soc. philomathique de Paris, (8), 4, 1891-2, 64-70.

$m-r$, while r digits precede the period. The condition that the length of the period be the maximum $\phi(b')$ is that 10 be a primitive root of b' , whence $b' = p^n$, since $b' \neq 4$ or $2p^n$, p being an odd prime.

P. Bachmann¹⁰¹ used a primitive root g of the prime p and set

$$\frac{g^{p-1}-1}{p} = Q = c_{p-2}g^{p-2} + \dots + c_1g + c_0,$$

to the base g . We get the multiples $Q, 2Q, \dots, (p-1)Q$ by cyclic permutation of the digits of Q . For $p=7, g=10, Q=142857$.

J. Kraus¹⁰² generalized the last result. When r_1/n is converted into a periodic fraction to base g , prime to n , let a_1, \dots, a_k be the quotients and r_1, \dots, r_k the remainders. Then

$$\frac{g^k-1}{n} r_\lambda = a_\lambda g^{k-1} + a_{\lambda+1} g^{k-2} + \dots + a_{\lambda-1} \quad (\lambda = 1, \dots, k),$$

whence

$$r_\lambda (a_1 g^{k-1} + \dots + a_k) = r_1 (a_\lambda g^{k-1} + \dots + a_{\lambda-1}).$$

In particular, let n be such that it has a primitive root g , and take $r_1=1$. Then

$$\frac{g^{\varphi(n)}-1}{n} = Q = a_1 g^{\varphi(n)-1} + a_2 g^{\varphi(n)-2} + \dots + a_{\varphi(n)},$$

and if r_λ is prime to n , the product $r_\lambda Q$ has the same digits as Q permuted cyclically and beginning with a_λ .

H. Brocard¹⁰³ gave a tentative method of factoring 10^n-1 .

J. Mayer¹⁰⁴ gave conditions under which the period of z/P to base a , where z and a are relatively prime to P , shall be complete, i. e., corresponding digits of the two halves of the period have the sum $a-1$.

Heinrich Bork¹⁰⁵ gave an exposition, without use of the theory of numbers, of known results on decimal fractions. There is here first published (pp. 36-41) a table, computed by Friedrich Kessler, showing for each prime $p < 100000$ the value of $q = (p-1)/e$, where e is the length of the period for $1/p$. The cases in which $q=1$ or 2 were omitted for brevity. He stated that there are many errors in the table to 15000 by Reuschle.⁴⁰ Cunningham¹²⁴ listed errata in Kessler's table.

L. E. Dickson¹⁰⁶ proved, without the use of the concept of periodic fractions, that every integer of D digits written to the base N , which is such that its products by D distinct integers have the same D digits in the same cyclic order, is of the form $A(N^D-1)/P$, where A and P are relatively prime. A number of this form is an integer only when P is prime

¹⁰¹Zeitschrift Math. Phys., 36, 1891, 381-3; Die Elemente der Zahlentheorie, 1892, 95-97.

A like discussion occurs in l'intermédiaire des math., 5, 1898, 57-8; 10, 1903, 91-3.

¹⁰²Zeitschrift Math. Phys., 37, 1892, 190-1.

¹⁰³El Progreso Matematico, 1892, 25-27, 89-93, 114-9. Cf. l'intermédiaire des math., 2, 1895, 323-4.

¹⁰⁴Zeitschrift Math. Phys., 39, 1894, 376-382.

¹⁰⁵Periodische Dezimalbrüche, Progr. 67, Prinz Heinrichs-Gymn., Berlin, 1895, 41 pp.

¹⁰⁶Quart. Jour. Math., 27, 1895, 366-77.

to N , and D is a multiple of the exponent d to which N belongs modulo P . The further discussion is limited to the case $D=d$, to exclude repetitions of the period of digits. Then the multipliers which cause a cyclic permutation of the digits are the least residues of N, N^2, \dots, N^D modulo P . For $A=1$, we have a solution for any N and any P prime to N . There are listed the 19 possible solutions with $A>1, N\leq 63$, and having the first digit >0 . The only one with $N=10$ is 142857. General properties are noted.

A like form is obtained (pp. 375-7) for an integer of D digits written to the base N , such that its quotients by D distinct integers have the same D digits in the same cyclic order. The divisors are the least residues of N^D, N^{D-1}, \dots, N modulo P . For example, if $N=11, P=7, A=4$, we get $4(11^3-1)/7$, or 631 to base 11, whose quotients by 2 and 4 are 316 and 163, to base 11. Another example is 512 to base 9.

E. Lucas¹ gave all the prime factors of 10^n-1 for $n\leq 18$.

F. W. Lawrence¹⁰⁷ proved that the large factors of $10^{25}-1$ and $10^{29}-1$ are primes.

C. E. Bickmore¹⁰⁸ gave the factors of $10^n-1, n\leq 100$. Here $(10^{23}-1)/9$ is marked prime on the authority of Loof, whereas the latter regarded its composition as unknown [Cunningham¹²³]. There is a misprint for 43037 in $10^{29}-1$.

B. Bettini¹⁰⁹ considered the number n of digits in the period of the decimal fraction for a/b , i. e., the exponent to which 10 belongs modulo b . If 10 is a quadratic non-residue of a prime b, n is even, but not conversely (p. 48). There is a table of values of n for each prime $b\leq 277$.

V. Murer¹¹⁰ considered the $n=mq$ remainders obtained when a/b is converted into a decimal fraction with a period of length n , separated them into sets of m , starting with a given remainder, and proved that the sum of the sets is a multiple of $9\dots 9$ (to m digits). Further theorems are found when $q=1, 2$ or 3 .

J. Sachs^{110a} tabulated all proper fractions with denominators <250 and their decimal equivalents.

B. Reynolds¹¹¹ repeated the rules given by Glaisher^{78,79} for the length of periods. He extended the rules by Sardi⁵³ and gave the number of times a given digit occurs in the various periods belonging to a denominator N , both for base 10 and other bases.

Reynolds¹¹² gave numerical results on periodic fractions for various bases the lengths of whose period is 3 or 6, and on the length of the period for $1/N$ for every base $<N-1$, when N is a prime.

A. Cunningham¹¹³ applied to the question of the length of the period of a periodic fraction to any base the theory of binomial congruences [see

¹⁰⁷Proc. London Math. Soc., 28, 1896-7, 465. Cf. Bickmore⁴⁹ of Ch. XVI.

¹⁰⁸Nouv. Ann. Math., (3), 15, 1896, 222-7.

¹⁰⁹Periodico di Mat., 12, 1897, 43-50.

¹¹⁰*Ibid.*, 142-150.

^{110a}Progr. 632, Baden-Baden, Leipzig, 1898.

¹¹¹Messenger Math., 27, 1897-8, 177-87.

¹¹²*Ibid.*, 28, 1898-9, 33-36, 88-91.

¹¹³*Ibid.*, 29, 1899-1900, 145-179. Errata.¹²³

201 of Ch. VII]. He gave extensive tables, and references to papers on higher residues and to tables relating to period lengths.

O. Fujimaki¹¹⁴ noted that if $10^m - 1$ is exactly divisible by n , and the quotient is $a_1 \dots a_m$ of m digits, the numbers obtained from the latter by cyclic permutations of the digits are all multiples of $a_1 \dots a_m$.

J. Cullen, D. Biddle, and A. Cunningham¹¹⁵ proved that the large factor of 14 digits of $(10^{25} + 1)/(10^5 + 1)$ is a prime.

L. Kronecker¹¹⁶ treated periodic fractions to any base.

W. P. Workman¹¹⁷ corrected three errors in Shanks'⁶¹ table.

D. Biddle¹¹⁸ concluded erroneously that $(10^{17} - 1)/9$ is a prime.

H. Hertzer¹¹⁹ extended Kessler's¹⁰⁵ table from 100000 to 112400, noted Reuschle's⁴⁰ error on the conditions that 10 be a biquadratic residue of a prime p and gave the conditions that 10 be a residue of an 8th power modulo p . For errata in the table, see Cunningham.¹²⁴

P. Bachmann¹²⁰ proved the chief results on periodic fractions and cyclic numbers to any base g .

A. Tagiuri¹²¹ proved theorems [F. Meyer,⁵⁴ Perkins²⁹] on purely periodic fractions to any base and on mixed fractions.

E. B. Escott¹²² noted a misprint in Bickmore's¹⁰⁸ table and two omissions in Lucas'⁹¹ table, but described inaccurately the latter table, as noted by A. Cunningham.¹²³

A. Cunningham¹²⁴ described various tables (cited above) which give the exponent to which 10 belongs, and listed many errata.

J. R. Akerlund¹²⁵ gave the prime factors of $11 \dots 1$ (to n digits) for $n \leq 16$, $n = 18$.

K. P. Nordlund¹²⁶ applied to periodic fractions the theorem that, if n_1, \dots, n_r are distinct odd primes, no one dividing a , then $N = n_1^{m_1} \dots n_r^{m_r}$ divides $a^k - 1$, where $k = \phi(N)/2^{r-1}$. He gave the period of $1/p$ for p a prime < 100 and of certain a/p .

T. H. Miller,¹²⁷ generalizing the fact that the successive pairs of digits in the period for $1/7$ are 14, 28, \dots , investigated numbers n to the base r for which

$$\frac{1}{n} = \frac{2n}{r^2} + \frac{4n}{r^4} + \frac{8n}{r^6} + \dots,$$

¹¹⁴Jour. of the Physics School in Tokio, 7, 1897, 16-21; Abh. Gesch. Math. Wiss., 28, 1910, 22.

¹¹⁵Math. Quest. Educat. Times, 72, 1900, 99-101.

¹¹⁶Vorlesungen über Zahlentheorie, I, 1901, 428-437.

¹¹⁷Messenger Math., 31, 1901-2, 115.

¹¹⁸*Ibid.*, p. 34; corrected, *ibid.*, 33, 1903-4, 126 (p. 95).

¹¹⁹Archiv Math. Phys., (3), 2, 1902, 249-252.

¹²⁰Niedere Zahlentheorie, I, 1902, 351-363.

¹²¹Periodico di Mat., 18, 1903, 43-58.

¹²²Nouv. Ann. Math., (4), 3, 1903, 136; Messenger Math., 33, 1903-4, 49.

¹²³Messenger Math., 33, 1903-4, 95-96.

¹²⁴*Ibid.*, 145-155.

¹²⁵Nyt Tidsskrift for Mat., Kjobenhavn, 16 A, 1905, 97-103.

¹²⁶Göteborgs Kungl. Vetenskaps-Handlingar, (4), VII-VIII, 1905.

¹²⁷Proc. Edinburgh Math. Soc., 26, 1907-8, 95-6.

whence $r^2 - 2n^2 = 2$. Besides the case $r=10$, $n=7$, he found $r=58$, $n=41$, etc.

A. Cunningham¹²⁸ noted two errors in his paper¹¹³ and added

$$252^{12} \equiv 1 \pmod{997^2}, \quad 390112^4 \equiv 1 \pmod{17^6}$$

and cases modulo p^2 , where $p=103, 487$, attributed to Th. Gosset.

A. Cunningham¹²⁹ gave tables of the periods of $1/N$ to the bases 2, 3, 5 for $N \leq 100$.

H. Hertzer¹³⁰ noted three errors in Bickmore's¹⁰⁸ table.

A. Gérardin¹³¹ gave factors of $10^n - 1$, $n < 100$, and a table of the exponents to which 10 belongs modulo p , a prime < 10000 , with a list of errors in the tables by Burckhardt and Desmarest.

A. Filippov¹³² gave two methods of determining the generating factor for the periodic fraction for $1/b$ (cf. Lucas, *Théorie des nombres*, p. 178).

G. C. Cicioni¹³³ treated the subject.

E. R. Bennett¹³⁴ proved the standard theorems by means of group theory.

W. H. Jackson¹³⁵ noted that, if a is prime to 10 and if b is chosen so that $b < 10$, $ab = 10m - 1$, the period for $1/a$ may be written as

$$b \{ 1 + 10m + (10m)^2 + \dots + (10m)^{s-1} \} - k \cdot 10^s,$$

where s is the exponent to which 10 belongs modulo a , and k is a positive integer. Thus for $a=39$, $b=1$, we have $m=4$, $s=6$, and the period is

$$1 + 40 + \dots + (40)^5 - k \cdot 10^6, \quad \frac{1}{39} = .\dot{0}2564\dot{1}.$$

G. Mignosi¹³⁶ discussed the logic underlying the identification of an unending decimal with its generator p/q .

A. Cunningham¹³⁷ treated periodic decimals with multiples having the same digits permuted cyclically.

F. Schuh¹³⁸ considered the length q_a of the period for $1/p^a$ for the base g , where p is a prime. He proved that q_a is of the form $q_1 p^c$, where $0 \leq c \leq a-2$ when $p=2$, $a > 2$, while $0 \leq c \leq a-1$ in all other cases. For $a > 2$,

$$q_{a-1} = q_1 p^{c-1}, \dots, \quad q_{a-c+1} = q_1 p, \quad q_{a-c} = \dots = q_2 = q,$$

where $q = q_1$ except when $p=2$, $g=4m-1$, and then $q=2$. Equality of periods for moduli p^a and p^b can occur for an odd prime p only when this period is q_1 , and for $p=2$ only when it is 1 or 2. It is shown how to find the numbers g which give equal periods for p^a and p , and the odd numbers g which give the period 2 for 2^a .

¹²⁸Math. Gazette, 4, 1907-8, 209-210. Sphinx-Oedipe, 8, 1913, 131.

¹²⁹Math. Gazette, 4, 1907-8, 259-267; 6, 1911-12, 63-7, 108-116.

¹³⁰Archiv Math. Phys., (3), 13, 1908, 107.

¹³¹Sphinx-Oedipe, Nancy, 1908-9, 101-112.

¹³²Spaczinskis Bote, 1908, pp. 252-263, 321-2 (Russian).

¹³³La divisibilità dei numeri e la teoria delle decimali periodiche, Perugia, 1908, 150 pp.

¹³⁴Amer. Math. Monthly, 16, 1909, 79-82.

¹³⁵Annals of Math., (2), 11, 1909-10, 166-8.

¹³⁶Il Boll. Matematica Gior. Sc.-Didat., 9, 1910, 128-138.

¹³⁷Math. Quest. Educat. Times, (2), 18, 1910, 25-26.

¹³⁸Nieuw Archief Wiskunde, (2), 9, 1911, 408-439. Cf. Schuh,¹²³⁻⁴, Ch. VII.

T. Ghezzi¹³⁹ considered a proper irreducible fraction m/p with p prime to the base b of numeration. Let b belong to the exponent n modulo p . In

$$mb = pq_1 + r_1, \quad r_1b = pq_2 + r_2, \dots, \quad 0 < r_1 < p, \quad 0 < r_2 < p, \dots,$$

r_1, \dots, r_n are distinct and $r_n = m$. Multiply the respective equations by b^{n-1}, b^{n-2}, \dots and add; we see that

$$\frac{m}{p} = \frac{q_1 b^{n-1} + \dots + q_n}{b^n - 1}.$$

A similar proof shows that m/p equals a fraction with the denominator $b^t(b^n - 1)$ when $b = a_1 a_2 a_3$, $p = p_1 a_1^r a_2^s a_3^t$, the a 's being primes and p_1 relatively prime to b , while b^t is the least power of b having the divisor $a_1^r a_2^s a_3^t$, and n is the exponent to which b belongs modulo p_1 .

F. Stasi¹⁴⁰ gave a long proof showing that the length of the period for b/a does not exceed that for $1/a$. If the period A for $1/p$ has m digits and $n = pq$ is prime to 10, the length of the period for $1/n$ is m if A is divisible by q ; is mi if A is prime to q and if the least $A(10^{m(k-1)} + \dots + 1)$ divisible by q has $m = i$; and is mj if $A = A'a$, $q = aq'$, with A' , q' relatively prime, while the least $A'(10^{m(k-1)} + \dots + 1)$ divisible by q' has $k = j$. For a prime $p \neq 2, 5$, let

$$\frac{1}{p^h} = \frac{A_h}{10^m - 1},$$

and let A_h be the first of the periods of successive powers of $1/p$ not divisible by p ; then the period for $1/p^{h+k}$ has mp^k digits. If p_i is a prime $\neq 2, 5$, and r_i is the length of the period for $1/p_i$, and if $1/p_i^{\beta_i}$ is the highest power of $1/p_i$ with a period of r_i digits, the length of the period for $1/p_i^{\alpha_i}$ is $r_i' = r_i p_i^{\alpha_i - \beta_i}$, and that for $1/\Pi p_i^{\alpha_i}$ is a multiple of the l. c. m. of the r_i' .

If n is prime to 10 and if $r_1, \dots, r_m = 1$ are the successive remainders on reducing $1/n$ to a decimal, then $r_i^2 \equiv r_{2i} \pmod{n}$. Hence if $1/n$ has a period of $2i$ digits, $r_i^2 \equiv 1 \pmod{n}$ and conversely. But if it has a period of $2i+1$ digits, $r_{i+1}^2 \equiv 10$ and conversely.

*K. W. Lichtenecker¹⁴¹ gave the length of the period for $1/p$, when p is a prime ≤ 307 , and the factors of $10^n - 1$, $n \leq 10$.

L. Pasternak¹⁴² noted that, after multiplying the terms of a fraction by 9, 3 or 7, we may assume the denominator $N = 10m - 1$. To convert R_0/N into a decimal, we have $10R_{k-1} = Ny_k + R_k$ ($k = 1, 2, \dots$). Set $R_k = 10z_k + e_k$, $e_k \leq 9$. Since $y_k \leq 9$, $e_k = y_k$ and $R_{k-1} = me_k + z_k$. Hence the successive digits of the period are the unit digits of the successive remainders.

E. Maillet¹⁴³ defined a unique development $a_0 + a_1/n + a_2/n^2 + \dots$ of an arbitrary number, where the a_i are integers satisfying certain conditions. He studied the conditions that the development be limited or periodic.

¹³⁹II Boll. Matematica Gior. Sc.-Didat., 9, 1910, 263-9.

¹⁴⁰Ibid., 11, 1912, 226-246.

¹⁴¹Zeitschr. für das Realschulwesen, 37, 1912, 338-349.

¹⁴²L'enseignement math., 14, 1912, 285-9.

¹⁴³L'intermédiaire des math., 20, 1913, 202-6.

Welsch¹⁴⁴ discussed briefly the length of the period of a decimal fraction.

B. Howarth¹⁴⁵ noted that D^2 is not a factor of $(10^{Dn}-1)/(10^n-1)$ if D is a prime and n is not a multiple of the length of the period for $1/D$. Again,¹⁴⁶ $(10^{mnp^2}-1)/9$ is not divisible by $(10^{mp}-1)(10^{np}-1)/81$.

A. Cunningham¹⁴⁷ factored $10^{99} \pm 1$. Known factors of $10^n \pm 1$ are given.

Cunningham¹⁴⁸ gave factors of $10^{mpn}-1$.

A. Leman¹⁴⁹ gave an elementary exposition and inserted proofs of Fermat's theorem and related facts, with the aim to afford a concrete introduction to the more elementary facts of the theory of numbers.

S. Weixer¹⁵⁰ would compute the period P for $1/p$ by multiplication, beginning at the right. Let c be the final digit of P , whence $pc=10z-1$. Then c is the first digit of the period P^1 for z/p . The units digit c_1 of $cz=10z_1+c_1$ is the tens digit of P and the units digit of P^1 . In $c_1z+z_1=10z_2+c_2$, c_2 is the hundreds digit of P and the tens digit of P^1 , etc.

A. Leman¹⁵¹ discussed the preceding paper.

Problems¹⁵² on decimal fractions may be cited here.

O. Hoppe¹⁵³ proved that $(10^{19}-1)/9$ is a prime.

M. Jenkins¹⁵⁴ noted that if $N=a^pb^q\dots$, where a, b, \dots are distinct primes $\neq 2, 5$, the period for $1/N$ is complementary (sum of corresponding digits of the half periods is 9) if and only if the lengths of the periods for $1/a, 1/b, \dots$ contain the same power of 2.

Kraitchik¹²⁵ of Ch. VII and Levänen³⁷ of Ch. XII gave tables of exponents to which 10 belongs. Bickmore and Cullen¹¹⁵ of Ch. XIV factored $10^{25}+1$.

FURTHER PAPERS INVOLVING NO THEORY OF NUMBERS.

J. L. Lagrange, *Leçons élém. à l'école normale en 1795*, Oeuvres 7, 200.

James Adams, *Annals Phil., Mag. Chem.* (Thompson), (2), 2, 1821, 16-18.

C. R. Telosius and S. Mörck, *Disquisitio. . . . Acad. Carolina, Lundae*, 1838 (*in Meditationum Math. . . . Publice Defendent C. J. D. Hill*, 1831, Pt. II).

J. A. Arndt, *Archiv Math. Phys.*, 1, 1841, 101-4.

J. Dienger, *ibid.*, 11, 1848, 232; *Jour. für Math.*, 39, 1850, 67.

Wm. Wiley, *Math. Magazine*, 1, 1882, 7-8.

A. V. Filippov, *Kagans Bote*, 1910, 214-221 (pedagogic).

¹⁴⁴*L'intermédiaire des math.*, 21, 1914, 10.

¹⁴⁵*Math. Quest. Educat. Times*, 28, 1915, 101-4.

¹⁴⁶*Ibid.*, 27, 1915, 33-4.

¹⁴⁷*Ibid.*, 29, 1916, 76, 88-9.

¹⁴⁸*Math. Quest. and Solutions*, 3, 1917, 59.

¹⁴⁹*Vom Periodischen Dezimalbruch zur Zahlentheorie*, Leipzig, 1916, 59 pp.

¹⁵⁰*Zeitschrift Math. Naturw. Unterricht*, 47, 1916, 228-230.

¹⁵¹*Ibid.*, 230-1.

¹⁵²*Zeitschrift Math. Naturw. Unterricht*, 12, 1881, 431; 20, 188; 23, 584.

¹⁵³*Proc. London Math. Soc., Records of Meeting*, Dec. 6, 1917, and Feb. 14, 1918, for a revised proof.

¹⁵⁴*Math. Quest. Educ. Times*, 7, 1867, 31-2. Minor results, 32, 1880, 69; 34, 1881, 97-8; 37, 1882, 44; 41, 1884, 113-4; 58, 1893, 108-9; 60, 1894, 128; 63, 1895, 34; 72, 1900, 75-6; 74, 1901, 35; (2), 2, 1902, 65-6, 84-5; 4, 1903, 29, 65-7, 95; 7, 1905, 97, 106, 109-10; 8, 1905, 57; 9, 1906, 73. *Math. Quest. and Solutions*, 3, 1917, 72 (table); 4, 1917, 22.



CHAPTER VII.

PRIMITIVE ROOTS, BINOMIAL CONGRUENCES.

PRIMITIVE ROOTS, EXPONENTS, INDICES.

J. H. Lambert¹ stated without proof that there exists a primitive root g of any given prime p , so that $g^e - 1$ is divisible by p for $e = p - 1$, but not for $0 < e < p - 1$.

L. Euler² gave a proof which is defective. He introduced the term primitive root and proved (art. 28) that at most n integers $x < p$ make $x^n - 1$ divisible by p , the proof applying equally well to any polynomial of degree n with integral coefficients. He stated (art. 29) that, for $n < p$, $x^n - 1$ has all n solutions "real" if and only if n is a divisor of $p - 1$; in particular, $x^{p-1} - 1$ has $p - 1$ solutions (referring to arts. 22, 23, where he repeated his earlier proof of Fermat's theorem). Very likely Euler had in mind the algebraic identity $x^{p-1} - 1 = (x^n - 1)Q$, from which he was in a position to conclude that Q has at most $n - p + 1$ solutions, and hence $x^n - 1$ exactly n . By an incomplete induction (arts. 32-34), he inferred that there are exactly $\phi(n)$ integers $x < p$ for which $x^n - 1$ is divisible by p , but $x^l - 1$ not divisible by p for $0 < l < n$, n being a divisor of $p - 1$ (as the context indicates). In particular, there exist $\phi(p - 1)$ primitive roots of p (art. 46). He listed all the primitive roots of each prime ≤ 37 .

J. L. Lagrange³ proved that, if p is an odd prime and

$$x^{p-1} - 1 = X\xi + pF,$$

where X, ξ, F are polynomials in x with integral coefficients, and if x^m and x^μ are the highest powers of x in X and ξ with coefficients not divisible by p , there are m integral values, numerically $< p/2$, of x which make X a multiple of p , and μ values making ξ a multiple of p . For, by Fermat's theorem, the left member is a multiple of p for $x = \pm 1, \pm 2, \dots, \pm (p-1)/2$, while at most m of these values make X a multiple of p and at most μ make ξ a multiple of p .

L. Euler⁴ stated that he knew no rule for finding a primitive root and gave a table of all the primitive roots of each prime ≤ 41 .

Euler⁵ investigated the least exponent x (when it exists) for which $fa^x + g$ is divisible by N . Find λ such that $-g = \lambda N$ is a multiple, say $a^\alpha r$, of a . Then $fa^{x-\alpha} - r$ is divisible by N . Set $r = \lambda' N = a^\beta s$, $\beta \geq 1$. Then $fa^{x-\alpha-\beta} - s$ is divisible by N ; etc. If the problem is possible, we finally get f as the residue of $fa^{x-\alpha-\dots-\zeta}$, whence $x = \alpha + \dots + \zeta$. For example, to find the least x for which $2^x - 1$ is divisible by $N = 23$, we have

$$1 + 23 = 2^3, \quad 3 - 23 = -2^5, \quad -5 - 23 = -2^7, \quad -7 + 23 = 2^4,$$

whence $x = 3 + 2 + 2 + 4 = 11$.

¹Nova Acta Eruditorum, Leipzig, 1769, p. 127.

²Novi Comm. Acad. Petrop., 18, 1773, 85; Comm. Arith., 1, 516-537.

³Nouv. Mém. Ac. Roy. Berlin, année 1775 (1777), p. 339; Oeuvres 3, 777.

⁴Opusc. Anal., 1, 1783 (1772), 121; Comm. Arith., 1, 506.

⁵Opusc. Anal., 1, 1783 (1773), 242; Comm. Arith., 2, p. 1; Opera postuma, I, 172-4.

A. M. Legendre⁶ started with Lagrange's³ result that, if p is a prime and n is a divisor of $p-1$,

$$(1) \quad x^n \equiv 1 \pmod{p}$$

has n incongruent integral roots. Let $n = \nu^\alpha \nu'^\beta \dots$, where ν, ν', \dots are distinct primes. A root a of (1) *belongs** to the exponent n if no one of $a^{\nu/\nu}, a^{\nu'/\nu'}, \dots$ is congruent to unity modulo p . For, if $a^\theta \equiv 1$, $0 < \theta < n$, let σ be the g. c. d. of θ, n , so that $\sigma = n\gamma - \theta z$ for integers γ, z ; then

$$a^{\theta z} \equiv 1, \quad a^\sigma \equiv a^{\theta z + \sigma} \equiv a^{n\gamma} \equiv 1,$$

contrary to hypothesis. Next, of the n roots of (1), n/ν satisfy $x^{n/\nu} \equiv 1 \pmod{p}$, and $n(1-1/\nu)$ do not. Likewise, $n(1-1/\nu')$ do not satisfy $x^{n/\nu'} \equiv 1$; etc. It is said to follow that there are

$$\phi(n) = n \left(1 - \frac{1}{\nu}\right) \left(1 - \frac{1}{\nu'}\right) \dots$$

numbers belonging to the exponent n modulo p . If

$$\beta^{\nu^\alpha} \equiv 1, \quad \beta^{\nu^{\alpha-1}} \not\equiv 1 \pmod{p},$$

β belongs to the exponent ν^α . If β' belongs to the exponent ν'^β , etc., the product $\beta\beta' \dots$ is stated to belong to the exponent n .

C. F. Gauss⁷ gave two proofs of the existence of primitive roots of a prime p . If d is a divisor of $p-1$, and a^d is the lowest power of a congruent to unity modulo p , a is said to belong to the exponent d modulo p . Let $\psi(d)$ of the integers $1, 2, \dots, p-1$ belong to the exponent d , a given divisor of $p-1$. Gauss showed that $\psi(d) = 0$ or $\phi(d)$, $\sum \psi(d) = p-1 = \sum \phi(d)$, whence $\psi(d) = \phi(d)$. In his second proof, Gauss set $p-1 = a^\alpha b^\beta \dots$, where a, b, \dots are distinct primes, proved the existence of numbers A, B, \dots belonging to the respective exponents a^α, b^β, \dots , and showed that $AB \dots$ belongs to the exponent $p-1$ and hence is a primitive root of p .

Let a be a primitive root of p , b any integer not divisible by p , and e the integer, uniquely determined modulo $p-1$, for which $a^e \equiv b \pmod{p}$. Gauss (arts. 57-59) called e the index of b for the modulus p relative to the base a , and wrote $e = \text{ind } b$. Thus

$$a^{\text{ind } b} \equiv b \pmod{p}, \quad \text{ind } bb' \equiv \text{ind } b + \text{ind } b' \pmod{p-1}.$$

Gauss (arts. 69-72) discussed the relations between indices for different bases and the choice of the most convenient base.

In articles 73-74, he gave a convenient tentative method for finding a primitive root of p . Form the period of 2 (the distinct least positive residues of the successive powers of 2); if 2 belongs to an exponent $t < p-1$, select a number $b < p$ not in the period of 2, and form the period of b ; etc.

If a belongs to the exponent t modulo p , the product of the terms in the period of a is $\equiv (-1)^{t+1} \pmod{p}$, while the sum of the terms is $\equiv 0$ unless $a \equiv 1$ (arts. 75, 79).

⁶Mém. Ac. R. Sc., Paris, 1785, 471-3. *Théorie des nombres*, 1798, 413-4; ed. 3, 1830, Nos. 341-2; German transl. by Maser, 2, pp. 17-18.

*This term was introduced later by Gauss.⁷

⁷Disquisitiones Arith., 1801, arts. 52-55.

The product of all the primitive roots of a prime $p \neq 3$ is $\equiv 1 \pmod{p}$; the sum of the primitive roots of p is $\equiv 0$ if $p-1$ is divisible by a square, but is $\equiv (-1)^n$ if $p-1$ is the product of n distinct primes (arts. 80, 81).

If p is an odd prime and e is the g. c. d. of $\phi(p^n) = p^{n-1}(p-1)$ and t , then $x^t \equiv 1 \pmod{p^n}$ has exactly e incongruent roots. It follows that there exist primitive roots of p^n , i. e., numbers belonging to the exponent $\phi(p^n)$ (arts. 85-89).

For $n > 2$, every odd number belongs modulo 2^n to an exponent which divides 2^{n-2} , so that primitive roots of 2^n are lacking; however, a modified method of employing indices to the base 5 may be used (arts. 90, 91).

If $m = A^a B^b \dots$, where A, B, \dots are distinct primes, and $\alpha = \phi(A^a)$, $\beta = \phi(B^b), \dots$, and if μ is the l. c. m. of α, β, \dots , then $z^\mu \equiv 1 \pmod{m}$ for z prime to m . Now $\mu < \alpha \cdot \beta \dots = \phi(m)$ except when $m = 2^n, p^n$ or $2p^n$, where p is an odd prime. Thus there exist primitive roots of m only when $m = 2, 4, p^n$ or $2p^n$ (art. 92).

Table I, at the end of Disq. Arith., gives on one page the indices of each prime $< p$ for each prime and power of prime modulus < 100 . Gauss gave no direct table to determine the number corresponding to a given index, but indicated (end of art. 316) how his Table III for the conversion of ordinary into decimal fractions leads to the number having a given index (cf. Gauss,^{15, 17} Ch. VI).

S. F. Lacroix⁸ reproduced Gauss' second proof of the existence of primitive roots of a prime, without a reference.

L. Poincot⁹ argued that the primitive roots of a prime p may be obtained from the algebraic expressions for the imaginary $(p-1)$ th roots of unity by increasing the numbers under the radical signs by such multiples of p that the radicals become integral. The $\phi(p-1)$ primitive roots of p may be obtained by excluding from $1, \dots, p-1$ the residues of the powers whose exponents are the distinct prime factors of $p-1$; while symmetrical, this method is unpractical for large p .

Frégier¹⁰ proved that the 2^n th power of any odd number has the remainder unity when divided by 2^{n+2} , if $n > 0$.

Poincot¹¹ developed the first point of his preceding paper. The equation for the primitive 18th roots of unity is $x^6 - x^3 + 1 = 0$. The roots are

$$x = a^i \sqrt[3]{\frac{1}{2}(1 + \sqrt{-3})}, \quad (a^3 = 1).$$

But $\sqrt{-3} \equiv \pm 4, \sqrt[3]{-7} \equiv 4, \sqrt[3]{-11} \equiv 2 \pmod{19}$. Thus the six primitive roots of 19 are $x = -4, 2, -9, -5, -6, 3$. In general, the algebraic expressions for the n th roots of unity represent the different integral roots of $x^n \equiv 1 \pmod{p}$, where p is a prime $kn+1$, after suitable integers are added to the numbers under the radical signs. Since unity is the only (integral)

⁸Complément des élémens d'algèbre, Paris, ed. 3, 1804, 303-7; ed. 4, 1817, 317-321.

⁹Mém. Sc. Math. et Phys. de l'Institut de France, 14, 1813-5, 381-392.

¹⁰Annales de Math. (ed., Gergonne), 9, 1818-9, 285-8.

¹¹Mém. Ac. Sc. de l'Institut de France, 4, 1819-20, 99-183.

root of $x^p \equiv 1 \pmod{p}$, if p is a prime > 2 , he concluded (p. 165) that p is a factor of the numbers under the radical signs in the formula for a primitive p th root of unity. Cf. Smith¹⁵⁹ of Ch. VIII.

Poinsot^{11a} again treated the same subject.

J. Ivory¹² stated that a primitive root of a prime p satisfies $x^{(p-1)/2} \equiv -1$, but no one of the congruences $x^t \equiv -1 \pmod{p}$, $t = (p-1)/(2a)$, where a ranges over the odd prime factors of $p-1$; while a number not a primitive root satisfies at least one of the $x^t \equiv -1$. Hence if each $a^t \not\equiv -1$ and $a^{(p-1)/2} \equiv -1$, then a is a primitive root.

V. A. Lebesgue¹³ stated that prior to 1829 he had given in the Bulletin du Nord, Moscow, the congruence $X \equiv 0$ of Cauchy¹⁴ for the integers belonging to the exponent n modulo p .

A. Cauchy¹⁴ proved the existence of primitive roots of a prime p , essentially as in Gauss' second proof. If $p-1$ is divisible by $n = a^\alpha b^\beta c^\gamma \dots$, where a, b, c, \dots are distinct primes, he proved that the integers belonging to the exponent n modulo p coincide with the roots of

$$X = \frac{(x^n - 1)(x^{n/ab} - 1)(x^{n/ac} - 1) \dots}{(x^{n/a} - 1)(x^{n/b} - 1) \dots (x^{n/abc} - 1) \dots} \equiv 0 \pmod{p}.$$

The roots of the equation $X = 0$ are the primitive n th roots of unity. For the above divisor n of $p-1$, the sum of the l th powers of the primitive roots of $x^n \equiv 1 \pmod{p}$ is divisible by p if l is divisible by no one of the numbers

$$n, n/a, n/b, \dots, n/ab, \dots, n/abc, \dots$$

But if several of these are divisors of l , and if we replace n, a, b, \dots by $\phi(n), 1-a, 1-b, \dots$ in the largest of these divisors in fractional form, we get a fraction congruent to the sum of the l th powers. In case $x^m \equiv 1 \pmod{p}$ has m distinct integral roots, the sum of the l th powers of all the roots is congruent modulo p to m or 0 , according as l is or is not a multiple of m .

M. A. Stern¹⁵ proved that the product of all the numbers belonging to an exponent d is $\equiv 1 \pmod{p}$, while their sum is divisible by p if d is divisible by a square, but is $\equiv (-1)^n$ if d is a product of n distinct primes (generalizations of Gauss, D. A., arts. 80, 81). If $p = 2n+1$ and a belongs to the exponent n , the product of two numbers, which do not occur in the period of a , occurs in the period of a . To find a primitive root of p when $p-1 = 2ab \dots$, where a, b, \dots are distinct odd primes, raise any number as 2 to the powers $(p-1)/a, (p-1)/b, \dots$; if no one of the residues modulo p is 1, the negative of the product of these residues is a primitive root of p ; in case one of the residues is 1, use 3 or 5 in place of 2. If $p = 2q+1$ and q are odd primes, 2 or -2 is a primitive root of p according as $p = 8n+3$ or $8n+7$. If $p = 4q+1$

^{11a}Jour. de l'école polytechnique, cah. 18, t. 11, 1820, 345-410.

¹²Supplement to Encyclopædia Britannica, 4, 1824, 698.

¹³Jour. de Math., 2, 1837, 258.

¹⁴Exercices de Math., 1829, 231; Oeuvres, (2), 9, 266, 278-90.

¹⁵Jour. für Math., 6, 1830, 147-153.

and q are primes, 2 and -2 are primitive roots of p . If $p=4q+1$ and $q=3n+1$ are primes, 3 and -3 are primitive roots of p .

F. Minding¹⁶ gave without reference Gauss' second proof of the existence of primitive roots of a prime.

F. J. Richelot¹⁷ proved that, if $p=2^m+1$ is a prime, every quadratic non-residue (in particular, 3) is a primitive root of p .

A. L. Crelle¹⁸ gave a table showing all prime numbers ≤ 101 having a given primitive root; also a table of the residues of the powers of the natural numbers when divided by the primes 3, ..., 101. His device¹⁹ for finding the residues modulo p of the powers of a will be clear from the example $p=7$, $a=3$. Write under the natural numbers <7 the residues of the successive multiples of 3 formed by successive additions of 3; we get

1	2	3	4	5	6
3	6	2	5	1	4.

Then the residues 3, 2, 6, ... of 3, 3^2 , 3^3 , ... modulo 7 are found as follows: after 3 comes the number 2 below 3 in the above table; after 2 comes the number 6 below 2 in the table; etc.

Crelle²⁰ proved that, if p is a prime and λ is prime to $p-1$ and $< p-1$, the residues modulo p of z^λ range with z over the integers 1, 2, ..., $p-1$. His proof that there exist $\phi(n)$ numbers belonging to the exponent n modulo p , if n divides $p-1$, is like that by Legendre.⁶

G. L. Dirichlet²¹ employed $\phi(k)$ systems of indices for a modulus $k=2^\lambda p^\pi p'^{\pi'} \dots$, where p, p', \dots are distinct primes, and $\lambda \geq 3$. Given any integer n prime to k , and primitive roots c, c', \dots of $p^\pi, p'^{\pi'}, \dots$, we can determine indices $\alpha, \beta, \gamma, \gamma', \dots$ such that

$$n \equiv (-1)^{\alpha\beta} \pmod{2^\lambda}, \quad n \equiv c^\gamma \pmod{p^\pi}, \quad n \equiv c'^{\gamma'} \pmod{p'^{\pi'}}, \dots$$

Michel Ostrogradsky²² gave for each prime $p < 200$ all the primitive roots of p and companion tables of the indices and corresponding numbers. (See Jacobi²³ and Tchebychev.³⁴)

C. G. J. Jacobi²³ gave for each prime and power of a prime < 1000 two companion tables showing the numbers with given indices and the index of each given number. In the introduction, he reproduced the table by Burckhardt, 1817, of the length of the period of the decimal fraction for $1/p$, for each prime $p \leq 2543$, and 22 higher primes. Of the 365 primes < 2500 , we therefore have 148 having 10 as a primitive root, and 73 of the form $4m+3$ having -10 as a primitive root. Use is made also of the primes for which 10 or -10 is the square or cube of a primitive root.

¹⁶Anfangsgründe der höheren Arith., 1832, 36-37.

¹⁷Jour. für Math., 9, 1832, p. 5.

¹⁸Ibid., 27-53.

¹⁹Also, *ibid.*, 28, 1844, 166.

²⁰Abh. Ak. Wiss. Berlin, 1832, Math., p. 57, p. 65.

²¹Ibid., 1837, Math., 45; Werke, 1, 1889, 333.

²²Lectures on alg. and transc. analysis, I-II, St. Pétersbourg, 1837; Mém. Ac. Sc. St. Pétersbourg, sér. 6, sc. math. et phys., 1, 1838, 359-85.

²³Canon Arithmeticus, Berlin, 1839, xl+248 pp. Errata, Cunningham.^{110,115}

To find a primitive root g of p , select any convenient integer a and form the residues of a, a^2, a^3, \dots [as by Crelle¹⁸]. Let n be the exponent to which a belongs. Set $nn' = p - 1$. If $n < p - 1$, select an integer b not in the period a, \dots, a^n . The residue of $b^{n'}$ is in this period of a . If b^f is the least power of b whose residue is in the period of a , then f divides n' , say $n' = ff'$ (p. xxiii). Since $a \equiv g^{n'}$, $b^f \equiv a^i$, we have

$$b^f \equiv g^{ff'i} \equiv g^{ff'i + nff'k}, \quad b \equiv g^{f'(i+nk)} \pmod{p},$$

for some value $0, 1, \dots, f-1$ of k . But k must be chosen so that $i+nk$ is prime to f . For, if $i+nk = du$, where d is a divisor of f , we would have $b^{f/d} \equiv a^u$. The nf residues of $a^r b^s$ ($r = 0, \dots, n-1$; $s = 0, \dots, f-1$) are distinct; their indices to base g are $f', 2f', \dots, nff'$ in some order and are known. If $nf' < p-1$, we employ an integer not in the set $a^r b^s$ and proceed similarly. Ultimately we obtain a primitive root and at the same time the index of every number. This method was used for the primes between 200 and 1000.

For primes < 200 , the tables by Ostrogradsky²² were reprinted with the same errors (noted at the end of the Canon).

Jacobi proved that, if n is an odd prime, any primitive root of n^2 is a primitive root of any higher power of n (p. xxxv).

For the modulus 2^μ , $4 \leq \mu \leq 9$, the final tables give the index I of any positive odd number to base 3, where

$$(-1)^{(N-1)(N-3)/8} N \equiv 3^I \pmod{2^\mu}.$$

Robert Murphy²⁴ stated the empirical theorem that every prime $an^2 + p$ has a as a primitive root if $p > a/2$, p is a prime $< a$, and if a is a primitive root of p . For example, a prime $10n^2 + 7$ has 10 as a primitive root.

H. G. Erlerus²⁵ considered two odd primes p and p' and a number m such that $m \equiv a \pmod{p}$, $m \equiv a' \pmod{p'}$. Let a belong to the exponent e modulo p , and a' to the exponent e' modulo p' . If δ is the g. c. d. of e and e' , then m belongs to the exponent ee'/δ modulo pp' . He discussed at length the number of integers belonging to the exponent n for a composite modulus.

A. Cauchy²⁶ called the least positive integer i for which $m^i \equiv 1 \pmod{n}$ the indicator relative (or corresponding) to the base m and modulus n , which are assumed relatively prime. If the base m is constant, and i_1, i_2 are the indicators corresponding to moduli n_1, n_2 , and if $n = n_1 n_2$ is prime to m , then the l. c. m. of i_1 and i_2 is the indicator corresponding to modulus n . If the modulus n is constant, and i_1, i_2 are the indicators corresponding to bases m_1, m_2 , and if i_1, i_2 are relatively prime, then $i_1 i_2$ is the indicator corresponding to the base $m_1 m_2$.

Let i_1, i_2 be the indicators corresponding to the bases m_1, m_2 and same modulus n . The g. c. d. ω of i_1, i_2 can be expressed (often in several ways) as a product uv such that $i_1/u, i_2/v$ are relatively prime. For, if $\omega = \alpha\beta \dots$,

¹⁸Phil. Mag., (3), 19, 1841, 369.

²²Elementa Doctrinæ Numerorum, Diss., Halis, 1841, 18-43.

²⁴Comptes Rendus Paris, 12, 1841, 824-845; Oeuvres, (1), 6, 124-146.

where α, β, \dots are powers of distinct primes, use α as a factor in forming u in case α is prime to i_1/α , but as a factor of v in case α is prime to i_2/α , and as a factor of either u or v indifferently in case α is prime to both i_1/α and i_2/α . Since i_1/u and i_2/v are relatively prime indicators corresponding to bases m_1^u and m_2^v , it follows from the preceding theorem that the indicator corresponding to base $m_1^u \cdot m_2^v$ and modulus n is

$$\frac{i_1}{u} \cdot \frac{i_2}{v} = \frac{i_1 i_2}{\omega} = \text{l. c. m. of } i_1, i_2.$$

Hence, given several bases m_1, m_2, \dots and a single modulus n , we can find a new base relative to which the indicator is the l. c. m. of the indicators corresponding to m_1, m_2, \dots . If the latter bases include all the integers $< n$ and prime to n , the corresponding indicators give all indicators which can correspond to modulus n , so that all of them divide a certain maximum indicator I . Then for every integer m relatively prime to n , $m^I \equiv 1 \pmod{n}$. If $n = \nu^a$, where ν is an odd prime, or if $n = 2$ or 4 , $I = \phi(n)$. If $n = 2^k$, $k > 2$, $I = \phi(n)/2$. If I_j is the maximum indicator corresponding to a power n_j of a prime, and if $n = \prod n_j$, then I is the l. c. m. of I_1, I_2, \dots . The equation $mx - ny = 1$ has the solution $x \equiv m^{I-1} \pmod{n}$.

Cauchy²⁷ republished the preceding paper, but with an extension from the limit $n = 100$ to the limit $n = 1000$ for his table of the maximum indicator I .

C. F. Arndt²⁸ gave (without reference) Gauss' second proof of the existence of a primitive root of an odd prime p , and proved the existence of the $\phi(p^n)$ primitive roots of p^n or $2p^n$, and that there are no primitive roots for moduli other than these and 4 . If t is a divisor of 2^{n-2} , $n > 2$, exactly t numbers belong to the exponent t modulo 2^n (p. 18). If, for a modulus p^n , $2p^n$, a belongs to the exponent t , then $a \cdot a^2 \dots a^t$ is congruent to $(-1)^{t+1}$ (pp. 26-27), while the product of the numbers belonging to the exponent t is congruent to $+1$ if $t \neq 2$ (pp. 37-38). He proved also Stern's¹⁵ theorem on the sum of these numbers. He gave the same two theorems also in a later paper.²⁹

L. Poinso³⁰ used the method of Legendre⁶ to prove the existence of $\phi(n)$ integers belonging to the exponent n , a divisor of $p-1$, where p is a prime. He gave (pp. 71-75) essentially Gauss' first proof, and gave his own⁹ method of finding primitive roots of a prime. The existence of primitive roots of p^n , $2p^n$, 4 , but of no further moduli, is established by use of the number of roots of binomial congruences (pp. 87-101).

C. F. Arndt³¹ noted that if a belongs to an even exponent t modulo 2^n , then $\pm a, \pm a^3, \dots, \pm a^{t-1}$ give the t incongruent numbers belonging to the exponent t , and are congruent to $k \cdot 2^{n-1} \pmod{2^n}$ ($k = 1, 3, 5, \dots$). The product of the numbers belonging to the exponent t modulo 2^n , $n > 2$, is $\equiv +1$.

²⁷Exercices d'Analyse et de Phys. Math., 2, 1841, 1-40; Oeuvres, (2), 12.

²⁸Archiv Math. Phys., 2, 1842, 9, 15-16.

²⁹Jour. für Math., 31, 1846, 326-8.

³⁰Jour. de Mathématiques, (1), 10, 1845, 65-70, 72.

³¹Archiv Math. Phys., 6, 1845, 395, 399.

E. Prouhet³² gave, without reference, Crelle's¹⁸ method of forming the residues of the powers of a number. The object of the paper is to give a uniform method of proof of theorems, given in various places in Legendre's text, relating to the residues of the first n powers of an integer belonging to the exponent n modulo P , especially when P is a prime or a power of a prime, and the existence of primitive roots. He gave (p. 658) the usual proof that ± 2 is a primitive root of a prime $2q+1$ if q is a prime $4k\pm 1$ (with a misprint).

C. F. Arndt³³ proved that if g is a primitive root of the odd prime p and if p^λ ($\lambda < n$) is the highest power of p dividing $G = g^{p-1} - 1$, then g belongs to the exponent $p^{n-\lambda}(p-1)$ modulo p^n . Conversely, if the last is true of a primitive root g of p , then G is divisible by p^λ and not by $p^{\lambda+1}$. The first result with $\lambda = 1$ shows that any primitive root of p^2 is a primitive root of p^n , $n > 2$. Let g be a primitive root of p ; if G is not divisible by p^2 , g is a primitive root of p^2 ; but if G is divisible by p^2 , and h is not divisible by p , then $g+hp$ is a primitive root of p^2 . Any odd primitive root of p^n is a primitive root of $2p^n$. If g is a primitive root of p^n or $2p^n$, and t is a divisor of $p^{n-1}(p-1)$, then if a ranges over the integers $< t$ and prime to t , the $\phi(t)$ integers belonging to the exponent t modulo p^n or $2p^n$ are g^e , where $e = p^{n-1}(p-1)a/t$. The numbers belonging to the exponent 2^{n-m} modulo 2^n are found more simply than by Gauss⁷ and Jacobi²³ (p. 37).

P. L. Tchebychef³⁴ proved that if α, β, \dots are the distinct prime factors of $p-1$, where p is a prime, then a is a primitive root of p if and only if no one of the congruences $x^\alpha \equiv a, x^\beta \equiv a, \dots \pmod{p}$ has an integral root. This furnishes a method (usually impracticable) of finding all primitive roots of p . A second method uses a number a belonging to the exponent n , and a number b not congruent to a power of a , and deduces a number belonging to an exponent $> n$. In the second supplement, he proved that 3 is a primitive root of any prime $2^{2n}+1$; that ± 2 is a primitive root of any prime $2a+1$ such that a is a prime $4k\pm 1$; 3 is a primitive root of $4N2^m+1$ if $m > 0$ and N is a prime $> 9^{2^m}/(4 \cdot 2^m)$; 2 is a primitive root of any prime $4N+1$ such that N is an odd prime. The last result was later proposed³⁵ as a question for solution (with reference to this text). There is given the table of primitive roots and indices for primes < 200 , due to Ostrogradsky²². Schapira (p. 314) noted that in the list of errata in Jacobi's²³ Canon (p. 222) there is omitted the error 8 for 6 in ind 14 for $p = 25$.

V. A. Lebesgue³⁶ remarked that Cauchy's¹⁴ congruence $X \equiv 0$ shows the existence of $\phi(n)$ integers belonging to the exponent n modulo p , a prime.

³²Nouv. Ann. Math., 5, 1846, 175-87, 659-62, 675-83.

³³Jour. für Math., 31, 1846, 259-68.

³⁴Theory of Congruences (in Russian), 1849. German translation by Schapira, Berlin, 1889, p. 192. Italian translation by Mlle. Massarini, Rome, 1895, with an extension of the tables of indices to 353.

³⁵Nouv. Ann. Math., 15, 1856, 353. Solved by use of Euler's criterion by P. H. Rochette, *ibid.*, 16, 1857, 159. Also proved by Desmarest,¹⁷ p. 278.

³⁶Nouv. Ann. Math., 8, 1849, 352; 11, 1852, 420.

E. Desmarest³⁷ devoted the last 86 pages of his book to primitive roots; the 70 pages claimed to be new might well have been reduced to five by the omission of trivial matters and the use of standard notations. To find (pp. 267-8) a primitive root of the prime $P = 6q + 1$, where q is an odd prime, seek an odd solution of $u^2 + 3 \equiv 0 \pmod{P}$ and set $u = 2R - 1$; then $R^3 \equiv -1$ and R belongs to the exponent 6; thus we know the solutions of $x^6 \equiv 1$; let a be any integer prime to P and not such a solution; if $a^q \equiv \pm 1$, then $\pm a$ belongs to the exponent q , and $\pm aR$ is a primitive root of P ; but, if $a^{2q} \not\equiv 1$, then $a^{3q} \equiv \mp 1 \pmod{P}$, and $\pm a$ is a primitive root of P . If $P = 8Q + 1$ and Q are primes, then $P \equiv 5 \pmod{12}$ and 3 is a quadratic non-residue and hence a primitive root of P .

Let P be a prime of the form $5q \pm 2$. Then $u^2 \equiv 5 \pmod{P}$ is not solvable. Thus, if a is a primitive root of P , $5 \equiv a^e$, where e is odd. Thus if e is prime to $P - 1$, 5 is a primitive root of P . It is recommended that 5 be the first number used in seeking by trial a primitive root. And yet he announced the theorem (p. 283) that 5 is in general a primitive root. If P is a prime $5q \pm 2$ also of the form $2^n Q + 1$, where Q is an odd prime including 1, then (pp. 284-6) 5 is a primitive root of P provided P is not a factor of $5^{2^n} - 1$. He gave the factors of the latter and of $10^{2^n} - 1$ for $n = 1, \dots, 5$.

Results, corresponding to those just quoted for 5, are stated for $\rho = 7, -7, 10, 17$. What is really given is a list of the linear forms of the primes P for which ρ is a quadratic non-residue. If, in addition, $P = 2^n Q + 1$, where Q is an odd prime, then ρ is a primitive root, provided $\rho^{2^n} \not\equiv 1 \pmod{P}$. The last condition is ignored in his statement of his results and again in his collection (pp. 297-8) of "principles which give primitive roots" entered in his table (pp. 298-300) giving a primitive root of each prime < 10000 .

V. A. Lebesgue³⁸ proved that, if a and $p = 2^i a + 1$ are primes, any quadratic non-residue x of p is a primitive root of p if

$$x^{2^{i-1}} + 1 \not\equiv 0 \pmod{p}.$$

J. P. Kulik³⁹ gave for each prime p between 103 and 353 the indices and all the primitive roots of p . His manuscript extended to 1000. There is an initial table giving the least primitive root of the primes from 103 to 1009.

G. Oltramare⁴⁰ called x a root of order or index m of a prime p if x belongs to the exponent $(p-1)/m$ modulo p . Let $X_m(x) \equiv 0 \pmod{p}$ be the congruence whose roots are exclusively the roots of order m of p . By changing x to $x^{1/n}$, we obtain $X_{mn} = \phi(x) \equiv 0$. If n_1, n_2, \dots, n are the divisors > 1 of n ,

$$X_m = \frac{\phi(x^n)}{X_{mn_1} \dots X_{mn}}$$

³⁷Théorie des nombres. Traité de l'analyse indéterminée du second degré à deux inconnues suivi de l'application de cette analyse à la recherche des racines primitives avec une table de ces racines pour tous les nombres premiers compris entre 1 et 10000, Paris, 1852, 308 pp. For errata, see Cunningham, *Mess. Math.*, 33, 1903, 145.

³⁸Nouv. Ann. Math., 11, 1852, 422-4.

³⁹Jour. für Math., 45, 1853, 55-81.

⁴⁰*Ibid.*, 303-9.

V. A. Lebesgue⁴¹ noted that, given a primitive root g ($g < p$) of the prime p , we can find at once the primitive roots of p^n . Let g' be the positive residue $< p^2$ when g^p is divided by p^2 and set $h = (g' - g)/p$. Then

$$g + px + p^2y \quad (y=0, \dots, p^{n-2}-1; x=0, \dots, p-1; x \neq h)$$

give $p^{n-2}(p-1)$ primitive roots. Replacing g by g^i , where i is less than and prime to $p-1$, we obtain $\phi\{\phi(p^n)\}$ primitive roots of p^n . In particular, a primitive root of p^2 is a primitive root of p^n (Jacobi²³). But, if $h=0$, g is not a primitive root of p^2 . Since

$$g^{\text{ind } a+e} \equiv p-a \pmod{p^n}, \quad e = \frac{1}{2}p^{n-1}(p-1),$$

we can reduce by half the size of Jacobi's Canon.

D. A. da Silva⁴² gave two proofs that $x^d \equiv 1 \pmod{p}$ has $\phi(d)$ primitive roots, if d divides $p-1$, and perfected the method of Poinset^{9,30} for finding the primitive roots of a prime.

F. Landry^{42a} was led to the same conclusion as Ivory.¹² In particular, if $p=2^k+1$, or if $p=2n+1$ (n an odd prime) and $a \neq p-1$, any quadratic non-residue a of p is a primitive root. For each prime $p < 10000$, at least one prime ≤ 19 is a quadratic non-residue of p . Cauchy's¹⁴ congruence for the primitive roots is derived and proved.

G. Oltramare⁴³ proved that $-3^a 2^{2\beta}$ is a primitive root of the prime $p=2a\beta+1$, if $a \neq 3$, $\beta \neq 3$, $3^{2a} \not\equiv 1$, $2^{2\beta} \not\equiv 1 \pmod{p}$; that, if

$$p=3 \cdot 2^m+1=q^2+3r^2, \quad qx+ry=1,$$

$(-1+qy-3rx)5^3/2$ is a primitive root of p ; and analogous theorems. If a and $2a+1$ are primes, 2 or a is a primitive root of $2a+1$, according as a is of the form $4n+1$ or $4n+3$. If a is a prime $\neq 3$ and if $p=2a+1$ is a prime and $m > 1$, then 3 is a primitive root of p unless $3^{2m-1}+1 \equiv 0 \pmod{p}$. [Cf. Smith.⁴⁷]

P. Buttel⁴⁴ attributed to Scheffler (Die unbestimmte Analytik, 1854, §142) the method of Crelle¹⁸ for finding the residues of powers.

C. G. Reuschle's⁴⁵ table C gives the Haupt-exponent (*i. e.*, exponent to which the number belongs) (a) of 10, 2, 3, 5, 6, 7 with respect to all primes $p < 1000$, and the least primitive root of p ; (b) of 10 and 2 for $1000 < p < 5000$ and a convenient primitive root; (c) of 10 for $5000 < p < 15000$ (no primitive root given). Numerous errata have been listed by Cunningham.¹¹⁰

Allegret⁴⁶ stated that if n is odd, n is not a primitive root of a prime $2^{2\lambda}n+1$, $\lambda > 0$; proof can be made as in Lebesgue.³⁸

⁴¹Comptes Rendus Paris, 39, 1854, 1069-71; same in Jour. de Math., 19, 1854, 334-6.

⁴²Propriedades geraes et resolucao directa das Congruencias binomias, Lisbon, 1854. Report by C. Alasia, Rivista di Fisica, Mat. e Sc. Nat., Pavia, 4, 1903, 25, 27-28; and Annaes Scientificos Acad. Polyt. do Porto, Coimbra, 4, 1909, 166-192.

^{42a}Troisième mémoire sur la théorie des nombres, Paris, 1854, 24 pp.

⁴³Jour. für Math., 49, 1855, 161-86.

⁴⁴Archiv Math. Phys., 26, 1856, 247.

⁴⁵Math. Abhandlung... Tabellen, Prog. Stuttgart, 1856; full title in the chapter on perfect numbers.¹⁰⁸

⁴⁶Nouv. Ann. Math., 16, 1857, 309-310.

H. J. S. Smith⁴⁷ stated that some of Oltramare's⁴³ general results are erroneous at least in expression, and gave a simple proof that $x^d \equiv 1 \pmod{p^n}$ has exactly d roots if d divides $\phi(p^n)$.

V. A. Lebesgue⁴⁸ proved that, if p is an odd prime and a, b belong to exponents α, β , there exist numbers belonging to the l. c. m. m of α, β , as exponent. Hence if neither α nor β is a multiple of the other, m exceeds α and β . If $d < p-1$ is the greatest of the exponents to which $1, \dots, p-1$ belong, the latter do not all belong to exponents dividing d , since otherwise they would give more than d roots of $x^d \equiv 1 \pmod{p}$. Hence there exist primitive roots of p . If a is odd, $\pm 1 + 2^a$ belongs to the exponent 2^{m-a} modulo 2^m (p. 87). If h belongs to the exponent k modulo p , a prime, then $h + Pz$ belongs modulo p^n to an exponent which divides kp^{n-1} (p. 101). If f is a primitive root of p , and $f^{p-1} - 1 = pz$, then f is a primitive root of p^n if and only if z is not divisible by p (p. 102).

G. L. Dirichlet⁴⁹ proved the last theorem and explained his²¹ system of indices for a composite modulus.

V. A. Lebesgue⁵⁰ published tables, constructed by J. Hoüel,⁵¹ of indices and corresponding numbers for each prime and power of prime modulus < 200 , which differ from Jacobi's²³ only in the choice of the least primitive root. There is an auxiliary table of the indices of $x!$ for prime moduli < 200 .

V. A. Lebesgue⁵² stated that, if $g < p$ is a primitive root of the prime p and if $g' \equiv g^{p-2} \pmod{p}$, then g' is a primitive root of p ; at least one of g and g' is a primitive root of p^n for n arbitrary.

V. Bouniakowsky⁵³ proved in a new way the theorems of Tchebychef³⁴ that 2 is a primitive root of $p = 8n+3$ if p and $4n+1$ are primes, and of $p = 4n+1$ if p and n are primes. He gave a method to find the exponent to which 2 or 10 belongs modulo p .

A. Cayley⁵⁴ gave a specimen table showing the indices α, β, \dots for every number $M \equiv a^\alpha b^\beta \dots \pmod{N}$, where $M < N$ and prime to N , for $N = 1, \dots, 50$. There is no apparent way of forming another single table for all N 's analogous to Jacobi's tables (one for each N) of numbers corresponding to given indices.

F. W. A. Heime⁵⁵ gave the least primitive root of each prime < 1000 . His other results are not new. A secondary root of a prime p is one belonging to an exponent $< p-1$ modulo p .

⁴⁷British Assoc. Report, 1859, 228; 1860, 120, §73; Coll. Math. Papers, 1, 50, 158 (Report on theory of numbers).

⁴⁸Introd. théorie des nombres, 1862, 94-96.

⁴⁹Zahlentheorie, §§128-131, 1863; ed. 2, 1871; ed. 3, 1879; ed. 4, 1894.

⁵⁰Mém. soc. sc. phys. et nat. de Bordeaux, 3, cah. 2, 1864-5, 231-274.

⁵¹Formules et tables numér., Paris, 1866. For moduli ≤ 347 .

⁵²Comptes Rendus Paris, 64, 1867, 1268-9.

⁵³Bull. Ac. Sc. St. Pétersbourg, 11, 1867, 97-123.

⁵⁴Quart. Jour. Math., 9, 1868, 95-96.

⁵⁵Untersuchungen, besonders in Bezug auf relative Primzahlen, primitive u. sekundäre Wurzeln, quadratische Reste u. Nichtreste; nebst Berechnung der kleinsten primitiven Wurzeln von allen Primzahlen zwischen 1 und 1000. Berlin, 1868; ed. 2, 1869.

C. J. D. Hill⁵⁶ noted that his tables of indices for the moduli 2^n and 5^n ($n \leq 5$) give the residues of numbers modulo 10^n , i. e., the last n digits. Using also tables for the moduli 9091 and 9901, as well as a table of logarithms, we are able to determine the last 22 digits.

B. M. Goldberg⁵⁷ gave the least primitive root of each prime < 10160 .

V. Bouniakowsky⁵⁸ proved that 3 is a primitive root of p if $p = 24n + 5$ and $(p-1)/4$ are primes; -3 is a primitive root of p if $p = 12n + 11$ and $(p-1)/2$ are primes; if ρ is a primitive root of the prime $p = 4n + 1$, one (or both) of ρ , $p - \rho$ is a primitive root of p^m and of $2p^m$; 5 is a primitive root of $p = 20n + 3$ or $20n + 7$ if p and $(p-1)/2$ are primes, and of $p = 40n + 13$ or $40n + 37$ if p and $(p-1)/4$ are primes; 6 is a primitive root of a prime $24n + 11$ and -6 of $24n + 23$ if $(p-1)/2$ is a prime; 10 is a primitive root of $p = 40n + 7$, 19, 23, and -10 of $p = 40n + 3$, 27, 39, if $(p-1)/2$ is a prime; 10 is a primitive root of a prime $80n + 73$, $n > 0$, or $80n + 57$, $n > 1$, if $(p-1)/8$ is a prime. If $p = 8an + 2a - 1$ or $8an + a - 2$ and $(p-1)/4$ are primes, and if $a^2 + 1$ is not divisible by p , a is a primitive root of p .

V. A. Lebesgue⁵⁹ proved certain theorems due to Jacobi²³ and the following theorem which gives a method different from Jacobi's for forming a table of indices for a prime modulus p : If a belongs to the exponent n , and if b is not in the period of a , and if f is the least positive exponent for which $b^f \equiv a^i$, then $x^f \equiv a$ has the root $a^i b^u$, where $ft + iu - 1 = nv$; the root belongs to the exponent nf if and only if u is prime to f .

Consider the congruence $x^m \equiv a \pmod{p}$, where a belongs to the exponent $n = (p-1)/n'$, and m is a divisor of n' . Every root r has a period of mn terms if no one of the residues of r , r^2, \dots, r^{m-1} is in the period of a . If all the prime divisors of m divide n , the m roots have a period of mn terms; but if m has prime divisors q, r, \dots , not dividing n , there are only

$$m \left(\frac{q-1}{q} \right) \left(\frac{r-1}{r} \right) \dots$$

roots having a period of mn terms. The existence of primitive roots follows; this is already the case if $m = n'$.

Mention is made of companion tables in manuscript giving indices of numbers, and numbers corresponding to indices, constructed by J. Ch. Dupain in full for $p < 200$, but from 200 to 1500 with reduction to one-half in view of $\text{ind } p - a \equiv \text{ind } a \pm (p-1)/2 \pmod{p-1}$.

L. Kronecker⁶⁰ proved the existence of two series of positive integers g_j, m_j ($j = 1, \dots, \rho$) such that the least positive residues modulo $k > 2$ of $g_1^{i_1} g_2^{i_2} \dots g_\rho^{i_\rho}$ give all the $\phi(k)$ positive integers $< k$ and prime to k , if $i_1 = 0, 1, \dots, m_1 - 1$; $i_2 = 0, 1, \dots, m_2 - 1$; etc. [cf. Mertens⁹²].

G. Barillari^{60a} proved that, if a is prime to b and belongs to the exponent

⁵⁶Jour. für Math., 70, 1869, 282-8; Acta Univ. Lundensis, Lund, 1, 1864 (Math.), No. 6, 18 pp.

⁵⁷Rest- und Quotient-Rechnung, Hamburg, 1869, 97-138.

⁵⁸Bull. Ac. Sc. St. Pétersbourg, 14, 1869, 375-81.

⁵⁹Comptes Rendus Paris, 70, 1870, 1243-1251.

⁶⁰Monatsber. Ak. Berlin, 1870, 881. Cf. Traub, Archiv Math. Phys., 37, 1861, 278-94.

^{60a}Giornale di Mat., 9, 1871, 125-135.

m modulo b , and if b^h is the highest power of b which divides $a^m - 1$, and if $n \geq h$, then b^n divides $a^e - 1$ where $e = mb^{n-h}$. Further, if b is a prime, a belongs to the exponent e modulo b^n . For a new prime b' , let m' , n' , h' have the corresponding properties. Then the exponent to which a belongs modulo $B = b^n b'^{n'}$. . . is the l. c. m. L of mb^{n-h} , $m'b'^{n'-h'}$, For $a = 10$, we see that L is the length of the period for the irreducible fraction N/B .

L. Sancier⁶¹ proved that if p is a prime and $a < p$ belongs to the exponent θ modulo p , there exists an infinitude of numbers $a + px = A$ such that $A^\theta - 1$ is divisible by p^k , but not by p^{k+1} , where k is any assigned positive integer. If A belongs to the exponent θ modulo $p > 2$, A will belong to the exponent θ modulo p^r if the highest power of p which divides $A^\theta - 1$ is $\geq p^r$; but if it be $p^{r-\delta}$, A belongs to the exponent θp^δ modulo p^r [Barillari^{60a}]. Hence A is a primitive root of p^r if a primitive root of p and if $A^{p-1} - 1$ is not divisible by p^2 , and there are $\phi\{\phi(p^r)\}$ primitive roots of p^r or $2p^r$. [Generalization of Arndt.³³]

C. A. Laisant⁶² noted that if a belongs to the exponent 3 modulo p , a prime, then $a + 1$ belongs to the exponent 6, and conversely. If a belongs to the exponent 6, $a + 1$ will not belong to the exponent 3 unless $p = 7$, $a = 3$. Hence if p is a prime $6m + 1$, there are two numbers a , b belonging to the exponent 3, and two numbers $a + 1$, $b + 1$ belonging to the exponent 6; also, $a + b = p - 1$. If (p. 399) $p + q$ is an odd prime and p is even, then $p^p q^q \equiv q$, $p^q q^p \equiv p \pmod{p + q}$.

G. Bellavitis^{62a} gave, for each power $p^i \leq 383$ of a prime p , the periodic fraction for $1/p^i$ to the base 2 and showed how to deduce the indices of numbers for the modulus p^i . Let $q = p^{i-1}(p - 1)$ and let 2 belong to the exponent q/r modulo p^i . A root b of $b^r \equiv 2 \pmod{p^i}$ is the base of the system of indices.

G. Frattini⁶³ proved by the theory of roots of unity that, if p is a prime, the number of interchanges necessary to pass from 1, 2, . . . , $p - 2$ to ind 2, ind 3, . . . , ind $(p - 1)$ and to

$$\text{ind } 1 - \text{ind } 2, \quad \text{ind } 2 - \text{ind } 3, \dots, \quad \text{ind } (p - 2) - \text{ind } (p - 1)$$

are both even or both odd.

Fritz Hofmann⁶⁴ used rotations of regular polygons to prove theorems on the sum of the primitive roots of a prime (Gauss⁷).

A. R. Forsyth⁶⁵ found the sum of the c th powers of the primitive roots of a prime p . The sum is divisible by p if $p - 1$ contains the square of a prime not dividing c or if it contains a prime dividing c but with an exponent exceeding by at least 2 its exponent in c . If neither of these conditions is satisfied, the result is not so simple.

⁶¹Bull. Soc. Math. de France, 4, 1875-6, 23-29.

⁶²Mém. Soc. Sc. Phys. et Nat. de Bordeaux, (2), 1, 1876, 400-2.

^{62a}Atti Accad. Lincei, Mem. Sc. Fis. Mat., (3), 1, 1876-7, 778-800.

⁶³Giornale di Mat., 18, 1880, 369-76.

⁶⁴Math. Annalen, 20, 1882, 471-86.

⁶⁵Messenger of Math., 13, 1883-4, 180-5.

J. Perott⁶⁶ gave a simple proof that $x^{p^k} \equiv 1 \pmod{p^n}$ has p^k roots. Thus there exists an integer b belonging to the exponent p^{n-1} modulo p^n . Assuming the existence of a primitive root of p , we employ a power of it and obtain a number a belonging to the exponent $p-1$ modulo p^n . Hence ab is a primitive root of p^n .

Schwartz⁶⁷ stated, and Hacken proved, the final theorem of Cauchy.¹⁴

L. Gegenbauer⁶⁸ stated 19 theorems of which a specimen is the following: If $p = 8a(8\beta + 1) + 24\beta + 5$ and $(p-1)/4$ are primes and if $64a^2 + 48a + 10$ is relatively prime to p , then $8a+3$ is a primitive root of p .

G. Wertheim⁶⁹ gave the least primitive root of each prime < 1000 and companion tables of indices and numbers for primes < 100 . He reproduced (pp. 125-130) arts. 80-81 of Gauss⁷ and stated the generalization by Stern.¹⁵

H. Kefenstein⁷⁰ would obtain all primitive roots of a prime p by excluding all residues of powers with exponents dividing $p-1$ [Poincot⁹].

M. F. Daniëls⁷¹ gave a proof like Legendre's⁶ that there are $\phi(n)$ numbers belonging to the exponent n modulo p , a prime, if n divides $p-1$.

*K. Szily⁷² discussed the "comparative number" of primitive roots.

E. Lucas⁷³ gave the name reduced indicator of n to Cauchy's²⁶ maximum indicator of n , and noted that it is a divisor $< \phi(n)$ of $\phi(n)$ except when $n=2, 4, p^k$ or $2p^k$, where p is an odd prime, and then equals $\phi(n)$. The exponent to which a belongs modulo m is called the "gaussien" of a modulo m (preface, xv, and p. 440).

H. Scheffler⁷⁴ gave, without reference, the theorem due to Richelot¹⁷ and the final one by Prouhet.³² To test if a proposed number a is a primitive root of a prime p , note whether p is of one of the linear forms of primes for which a is a quadratic non-residue, and, if so, raise a to the powers whose exponents divide $(p-1)/2$.

L. Contejean⁷⁵ noted that the argument in Serret's *Algèbre*, 2, No. 318, leads to the following result [for the case $a=10$]: If p is an odd prime and a belongs to the exponent $e = (p-1)/q$ modulo p , it belongs to the exponent $p^{r-1}e$ modulo p^r when $(a^e - 1)/p$ is not divisible by p , but to a smaller exponent if it is divisible by p [Sancery⁶¹].

P. Bachmann⁷⁶ proved the existence of a primitive root of a prime p by use of the group of the residues $1, \dots, p-1$ under multiplication.

⁶⁶Bull. des Sc. Math., 9, I, 1885, 21-24. For $k=n-1$ the theorem is contained implicitly in a posthumous fragment by Gauss, Werke, 2, 266.

⁶⁷Mathesis, 6, 1886, 280; 7, 1887, 124-5.

⁶⁸Sitzungsber. Ak. Wiss. Wien (Math.), 95, II, 1887, 843-5.

⁶⁹Elemente der Zahlentheorie, 1887, 116, 375-381.

⁷⁰Mitt. Math. Gesell. Hamburg, 1, 1889, 256.

⁷¹Lineaire Congruenties, Diss., Amsterdam, 1890, 92-99.

⁷²Math. és termes értesítő (Memoirs Hungarian Ac. Sc.), 9, 1891, 264; 10, 1892, 19. Magyar Tudom. Ak. Ertesitoje (Report of Hungarian Ac. Sc.), 2, 1891, 478.

⁷³Théorie des nombres, 1891, 429.

⁷⁴Beiträge zur Zahlentheorie, 1891, 135-143.

⁷⁵Bull. Soc. Philomathique de Paris, (8), 4, 1891-2, 66-70.

⁷⁶Die Elemente der Zahlentheorie, 1892, 89.

G. B. Mathews⁷⁷ reproduced art. 81 of Gauss⁷ and gave a second proof by use of Cauchy's¹⁴ congruence $X \equiv 0$ for $n = p - 1$.

K. Zsigmondy⁷⁸ treated the problem to find all integers K , relatively prime to given integers a and b , such that $a^\sigma \equiv b^\sigma \pmod{K}$ holds for the given integral value $\sigma = \gamma$, but for no smaller value. For $b = 1$, it is a question of the moduli K with respect to which a belongs to the exponent γ . Set $\gamma = \Pi q_i^{\alpha_i}$, where the q 's are distinct primes and q_1 the greatest. Then all the primes K for which $a^\sigma \equiv b^\sigma \pmod{K}$ holds for $\sigma = \gamma$, but for no smaller σ , coincide with the prime factors of

$$\Delta = \frac{(a^\gamma - b^\gamma) \Pi (a^{\frac{\gamma}{q_1}} - b^{\frac{\gamma}{q_1}}) \dots}{\Pi (a^{\gamma/q} - b^{\gamma/q}) \dots},$$

in which the products extend over the combinations of q_1, q_2, \dots one, two, ... at a time, provided that, if $a^\sigma \equiv b^\sigma \pmod{q_1}$ for $\sigma = \gamma/q_1^{\alpha_1}$, but for no smaller σ , we do not include among the K 's the prime q_1 , which then occurs in Δ to the first power only. If the prime p is a K and if p^e is the highest power of p dividing Δ , then p^e is the highest power of p giving a K . The composite K 's are now easily found. If a and b are not both numerically equal to unity, it is shown that there is at least one prime K except in the following cases: $\gamma = 1$, $a - b = 1$; $\gamma = 2$, $a + b = \pm 2^\mu$ ($\mu \geq 1$); $\gamma = 3$, $a = \pm 2$, $b = \mp 1$; $\gamma = 6$, $a = \pm 2$, $b = \pm 1$. The case $b = 1$ shows that, apart from the corresponding exceptions, there exists a prime with respect to which the given integer $a \neq \pm 1$ belongs to the given exponent γ . As a corollary, every arithmetical progression of the type $\mu\gamma + 1$ ($\mu = 1, 2, \dots$) contains an infinitude of primes.

Zsigmondy⁷⁹ considered the function $\Delta_\gamma(a)$ obtained from the above Δ by setting $b = 1$. If a is a primitive root of the prime $p = 1 + \gamma$, the main theorem of the last paper shows that p divides $\Delta_\gamma(a)$. Conversely, $1 + \gamma$ is a prime if it divides Δ . Thus, if all the primes of a set of integers possess the same primitive root a , any integer p of the set is a prime if and only if $\Delta_{p-1}(a)$ is divisible by p . Hence theorems due to Tchebychef³⁴ imply criteria for primes. For example, a prime $2^{2n} + 1$ has the primitive root 3 implies that $2^{2n} + 1$ is a prime if and only if it divides $3^k + 1$, where $k = 2^{2n}$. Since ± 2 is a primitive root of any prime $2q + 1$ such that q is a prime $4k \pm 1$, we infer that, if q is a prime $4k \pm 1$, then $2q + 1$ is a prime if and only if it divides $(2^q \pm 1)/(2 \pm 1)$. Since 2 is a primitive root of a prime $4N + 1$ such that N is an odd prime, we infer that, if N is an odd prime, $4N + 1$ is a prime if and only if it divides $(2^{2N} + 1)/5$.

G. F. Bennett⁸⁰ proved (pp. 196-7) the first theorem of Cauchy,²⁶ and (pp. 199-201) the results of Sancery.⁶¹ If a and a' belong to exponents t and t' which contain no prime factor raised to the same power in each, then the exponent to which aa' belongs is the l. c. m. of t and t' (p. 194).

⁷⁷Theory of Numbers, 1892, 23-25.

⁷⁸Monatshefte Math. Phys., 3, 1892, 265-284.

⁷⁹*Ibid.*, 4, 1893, 79-80.

⁸⁰Phil. Trans. R. Soc. London, 184 A, 1893, 189-245.

If 2^{s+1} is the highest power of 2 dividing $a^2 - 1$, where a is odd, the exponent to which a belongs modulo 2^λ is $2^{\lambda-s}$ if $\lambda > s$, but, if $\lambda \leq s$, is 1 if $a \equiv 1$, 2 if $a^2 \equiv 1$, $a \not\equiv 1 \pmod{2^\lambda}$; the result of Lebesgue⁴⁸ (p. 87) now follows (pp. 202-6). In case a is not prime to the modulus, there is an evident theorem on the earliest power of a congruent to a higher power (p. 209). If e is a given divisor of $\phi(m)$, there is determined the number of integers belonging to exponent e modulo m [cf. Erlerus²⁵]. If a, a', \dots belong to the exponents t, t', \dots and if no two of the $tt' \dots$ numbers $a^r a'^{r'} \dots$ ($0 \leq r < t, 0 \leq r' < t', \dots$) are congruent modulo m , then a, a', \dots are called independent generators of the $\phi(m)$ integers $< m$ and prime to m (p. 195); a particular set of generators is given and the most general set is investigated (pp. 220-241) [a special problem on abelian groups].

J. Perott⁸¹ found a number belonging to an exponent which is the l. c. m. of the exponents to which given numbers belong. If, for a prime modulus p , a belongs to an exponent $t > 1$, and b to an exponent which divides t , then b is congruent to a power of a (proof by use of Newton's relations between the sums of like powers of a, \dots, a' and their elementary symmetric functions). Hence there exists a primitive root of p .

M. Frolov⁸² noted that all the quadratic non-residues of a prime modulus m are primitive roots of m if $m = 2^{2c} + 1$, $m = 2n + 1$ or $4n + 1$ with n an odd prime [Tchebychef³⁴]. To find primitive roots of m "without any trial," separate the $m - 1$ integers $< m$ into sets of fours $a, b, -a, -b$, where $ab \equiv 1 \pmod{m}$: Begin with one such set, say 1, 1, -1, -1. Either a or $m - a$ is even; divide the even one by 2 and multiply the corresponding $\pm b$ by 2; we get another set of four. Repeat the process. If the resulting series of sets contains all $m - 1$ integers $< m$, 2 and -2 are primitive roots if $m = 4h + 1$, and one of them is a primitive root if $m = 4h - 1$. If the sets just obtained do not include all $m - 1$ integers $< m$, further theorems are proved.

G. Wertheim⁸³ gave the least primitive root of each prime $p < 3000$.

L. Gegenbauer^{83a} gave two expressions for the sum s_k of those terms of a complete set of residues modulo p which belong to the exponent k , and evaluated $\sum s_{k/t} f(t)$ with t ranging over the divisors of k .

G. Wertheim⁸⁴ proved that any prime $2^{4n} + 1$ has the primitive root 7. If $p = 2^n q + 1$ is a prime and q is a prime > 2 , any quadratic non-residue m of p is a primitive root of p if $m^{2^n} - 1$ is not divisible by p . As corollaries, we get primes q of certain linear forms for which 2, 5, 7 are primitive roots of a prime $2q + 1$ or $4q + 1$; also, 3 is a primitive root of all primes $8q + 1$ or $16q + 1$ except 41; and cases when 5 or 7 is a primitive root of primes $8q + 1$, $16q + 1$. There is given a table showing the least primitive root of each prime between 3000 and 3500.

⁸¹Bull. des Sc. Math., (2), 17, I, 1893, 66-83.

⁸²Bull. Soc. Math. de France, 21, 1893, 113-128; 22, 1894, 241-5.

⁸³Acta Mathematica, 17, 1893, 315-20; correction, 22, 1899, 200 (10 for $p = 1021$).

^{83a}Denkschr. Ak. Wiss. Wien (Math.), 60, 1893, 48-60.

⁸⁴Zeitschrift Math. Naturw. Unterricht, 25, 1894, 81-97.

J. Perott⁸⁵ employed the sum s_k of the k th powers of $1, 2, \dots, p-1$, and gave a new proof that $s_1 \equiv 0, \dots, s_{p-2} \equiv 0, s_{p-1} \equiv -1 \pmod{p}$. If m is the l. c. m. of the exponents to which $1, 2, \dots, p-1$ belong, evidently $s_m \equiv p-1$, whence $m > p-2$. If A belongs to the exponent m , then A, A^2, \dots, A^m are incongruent, whence $m \leq p-1$. Thus A is a primitive root.

N. Amici⁸⁶ proved that, if $\nu > 2$, a number belongs to the exponent $2^{\nu-2}$ modulo 2^ν if and only if it is of the form $8h \pm 3$, and called such numbers quasi primitive roots of 2^ν . For a base $8h \pm 3$, numbers of the two forms $8k+1$ or $8k \pm 3$, and no others, have indices. The product of two numbers having indices has an index which is congruent modulo $2^{\nu-2}$ to the sum of the indices of the factors. The product of two numbers b_1 and b_2 , neither with an index, has an index congruent modulo $2^{\nu-2}$ to the sum of the indices of $-b_1$ and $-b_2$. The product of a number with an index by one without an index has no index.

K. Zsigmondy⁸⁷ proved by use of abelian groups that, if $\delta = q_1^{k_1} \dots q_r^{k_r}$, $m = p_1^{\pi_1} \dots p_s^{\pi_s}$, where q_1, \dots, q_r are distinct primes, and p_1, \dots, p_s are distinct primes, the number of incongruent integers belonging to the exponent δ modulo m is

$$\delta_1 \dots \delta_s \prod_{i=1}^r (1 - 1/q_i^{l_i}),$$

where δ_j is the g. c. d. of δ and $t_j = \phi(p_j^{\pi_j})$, while l_i is the number of the integers t_1, \dots, t_s which contain the factor $q_i^{k_i}$.

E. de Jonquières⁸⁸ proved that the product of an even number of primitive roots of a prime p is never a primitive root, while the product of an odd number of them is either a primitive root or belongs to an exponent not dividing $(p-1)/2$. Similar results hold for products of numbers belonging to like exponents. Certain of the n integers r , for which r^n is a given number belonging to the exponent $e = (p-1)/n$, belong to the exponent ne , while the others (if any are left) belong to an exponent ke , where k divides n . He conjectured that 2 is not a primitive root of a prime $p \equiv 1, 7, 17$ or $23 \pmod{24}$; 3 not of $p \equiv 1, 11, 13$ or $23 \pmod{24}$; 5 not of $p \equiv 1, 11, 19$, or $29 \pmod{30}$. These results and analogous ones for 7 and 11 were shown by him and T. Pepin⁸⁹ to follow from the quadratic reciprocity law and Gauss' theorems on the divisors of $x^2 \pm A$.

G. Wertheim⁹⁰ added to his⁸⁴ corollaries cases when 6, 10, 11, 13 are primitive roots of primes $2q+1, 4q+1$; also, 10 is a primitive root of all primes $8q+1 \neq 137$ for which q is a prime $10k+7$ or $10k+9$, and of primes $16q+1$ for which q is a prime $10k+1$ or $10k+7$.

Wertheim⁹¹ gave the least primitive root of each prime between 3000 and 5000 and of certain higher primes. He noted errata in his⁸³ table to 3000.

⁸⁵Bull. des Sc. Mathématiques, 18, I, 1894, 64-66.

⁸⁶Rendiconti Circolo Mat. di Palermo, 8, 1894, 187-201.

⁸⁷Monatshefte Math. Phys., 7, 1896, 271-2.

⁸⁸Comptes Rendus Paris, 122, 1896, p. 1451, p. 1513; 124, 1897, p. 334, p. 428.

⁸⁹Comptes Rendus Paris, 123, 1896, pp. 374, 405, 683, 737.

⁹⁰Acta Math., 20, 1896, 143-152.

⁹¹Ibid., 153-7; corrections, 22, 1899, 200.

F. Mertens⁹² called i_1, \dots, i_p the system of indices of n modulo k if $n \equiv g_1^{i_1} \dots g_p^{i_p} \pmod{k}$ for the g 's of Kronecker.⁶⁰ Such systems of indices differ from Dirichlet's.

C. Moreau⁹³ set $N = p^k q^h \dots$, $\nu = p^{k-1} q^{h-1} \dots$, where p, q, \dots are distinct primes. Take $\epsilon = 1$ if N is not divisible by 4 or if $N = 4$, but $\epsilon = 2$ if N is divisible by 4 and $N > 4$. Let $\psi(N)$ denote the l. c. m. of $\nu/\epsilon, p-1, q-1, \dots$ [equivalent to Cauchy's²⁶ maximum indicator for modulus N]. For A prime to N , $A^{\psi(N)} \equiv 1 \pmod{N}$. If $N = p^k, 2p^k$ or 4 (so that N has primitive roots), $\psi(N) = \phi(N)$ [Lucas⁷³]. There is a table of values of $N < 1000$ and certain higher values for which $\psi(N)$ has a given value < 100 .

A. Cunningham⁹⁴ noted that we may often abbreviate Gauss' method of finding a primitive root of a prime p by testing whether or not the trial root a is a primitive root before computing the residues of all powers of a . The tests are the simple rules to decide whether or not a is a quadratic or cubic residue of p . If a is both a quadratic non-residue and a cubic non-residue of $p = 3\omega + 1$, and if $a^f \not\equiv 1$ for every f dividing $p-1$ except $f = p-1$, then a is a primitive root.

A. Cunningham⁹⁵ gave tables showing the residues of the successive powers of 2 when divided by each prime or power of prime < 1000 , also companion tables showing the indices x of 2^x whose residues modulo p^k are 1, 2, 3, \dots . The tables are more convenient than Jacobi's Canon²³ (errata given here) for the problem to find the residue of a given number with respect to a given power of a prime, but less convenient for finding all roots of a given order of a given prime. There are given (p. 172) for each power $p^k < 1000$ of a prime p the factors of $\phi(p^k)$, the exponent ξ to which 2 belongs modulo p^k , and the quotient ϕ/ξ .

E. Cahen⁹⁶ proved that if p is a prime $> (3^{2^{m+1}} - 1)/2^{m+3}$ and if $q = 2^{m+2}p + 1$ ($m > 0$) is a prime, then 3 is a primitive root of q , whereas Tchebychef³⁴ had the less advantageous condition $p > 3^{2^{m+1}}/2^{m+2}$. Other related theorems by Tchebychef are proved. There are companion tables of indices for primes < 200 .

G. A. Miller⁹⁷ applied the theory of groups to prove the existence of primitive roots of p^n , to show that the primitive roots of p^2 are primitive roots of p^n , and to determine primitive roots of the prime p .

L. Kronecker⁹⁸ discussed the existence of primitive roots, defined systems of indices and applied them to the decomposition of fractions into partial fractions. He developed (pp. 375-388) the theory of exponents to which numbers belong modulo p , a prime, by use of the primitive factor

⁹²Sitzungsber. Ak. Wien (Math.), 106, II a, 1897, 259.

⁹³Nouv. Ann. Math., (3), 17, 1898, 303.

⁹⁴Math. Quest. Educat. Times, 73, 1900, 45, 47.

⁹⁵A Binary Canon, showing residues of powers of 2 for divisors under 1000, and indices to residues, London, 1900, 172 pp. Manuscript was described by author, Report British Assoc., 1895, 613. Errata, Cunningham.¹³⁵

⁹⁶Éléments de la théorie des nombres, 1900, 335-9, 375-390.

⁹⁷Bull. Amer. Math. Soc., 7, 1901, 350.

⁹⁸Vorlesungen über Zahlentheorie, I, 1901, 416-428.

$F_d(x)$ of $x^d - 1$ (dividing the last but not $x^t - 1$ for $t < d$). To every divisor d of $p-1$ belong exactly $\phi(d)$ numbers which are the roots of $F_d(x) \equiv 0 \pmod{p}$.

P. G. Foglini⁹⁹ gave an exposition of known results on primitive roots, indices, linear congruences, etc. In applying (p. 322) Poinso't's⁹ method of finding the primitive roots of a prime p to the case $p = 13$, it suffices to exclude the residues of the cubes of the numbers which remain after excluding the residues of squares; for, if x is a residue of a square, $(x^3)^6 \equiv 1$ and x^3 is the residue of a square.

R. W. D. Christie¹⁰⁰ noted that, if γ is a primitive root of a prime $p = 4k - 1$, the remaining primitive roots are congruent to $p - \gamma^{2^n}$ ($n = 1, 2, \dots$)

A. Cunningham¹⁰¹ noted that 3, 5, 6, 7, 10 and 12 are primitive roots of any prime $F_n = 2^{2^n} + 1 > 5$. Also $F_n^{2^{n+2}} + 1 \equiv 0 \pmod{F_{n+1} > 5}$.

E. I. Grigoriev¹⁰² noted that a primitive root of a prime p can not equal a product of an even number of primitive roots [evident].

G. Wertheim¹⁰³ treated the problem to find the numbers belonging to the exponent equal to the l. c. m. of m, n , given the numbers belonging to the exponents m and n , and proved the first theorem of Stern.¹⁵ He discussed (pp. 251-3) the relation between indices to two bases and proved (pp. 258, 402-3) that the sum of the indices of a number for the various primitive roots of $m = p^n$ or $2p^n$ equals $\frac{1}{2}\phi(m)\phi\{\phi(m)\}$. If a belongs to the exponent 4δ modulo p , the same is true of $p - a$ (p. 266). He gave a table showing the least primitive root of each prime < 6200 and for certain larger primes; also tables of indices for primes < 100 .

P. Bachmann¹⁰⁴ gave a generalization (corrected on p. 402) of Stern's¹⁵ first theorem.

G. Arnoux¹⁰⁵ constructed tables of residues of powers and tables of indices for low composite moduli.

A. Bindoni¹⁰⁶ noted that a table showing the exponent to which a belongs modulo p , a prime, can be extended to a table modulo N by means of the following theorems. Let a, b_1, \dots, b_n be relatively prime by twos. A number belonging to the exponent t_i modulo b_i belongs modulo $b_1 b_2 \dots b_n$ to the l. c. m. of t_1, \dots, t_n as exponent. If t_i is the least exponent for which $a^{t_i} + 1 \equiv 0 \pmod{b_i}$ and if the t_i are all odd, the least t for which $a^t + 1$ is divisible by b_1, \dots, b_n is the l. c. m. of t_1, \dots, t_n . If p is an odd prime not dividing a and if a belongs to the exponent t modulo p , and $a^t = pq + 1$, and if p^u is the highest power of p dividing q , then a belongs to the exponent tp^{n-1-u} modulo p^n . Hence if a is a primitive root of p , it is one of p^n if

⁹⁹Memorie Pont. Ac. Nuovi Lincei, 18, 1901, 261-348.

¹⁰⁰Math. Quest. Educat. Times, 1, 1902, 90.

¹⁰¹*Ibid.*, pp. 108, 116.

¹⁰²Kazani Izv. fiz. mat. obsc., Bull. Phys. Math. Soc. Kasan, (2), 12, 1902, No. 1, 7-10.

¹⁰³Anfangsgründe der Zahlenlehre, 1902, 236-7, 259-262.

¹⁰⁴Niedere Zahlentheorie, 1, 1902, 333-6.

¹⁰⁵Assoc. franç. av. sc., 32, 1903, II, 65-114.

¹⁰⁶Il Boll. di Matematica Giorn. Sc. Didat., Bologna, 4, 1905, 88-92.

and only if $a^{p-1} - 1$ is not divisible by p^2 . If t is even, the least x for which $a^x + 1 \equiv 0 \pmod{p^n}$ is $\frac{1}{2}tp^{n-1-u}$.

M. Cipolla¹⁰⁷ gave a historical report on congruences (especially binomial), primitive roots, exponents, indices (in Peano's symbolism).

K. P. Nordlund¹⁰⁸ proved by use of Fermat's theorem that, if n_1, \dots, n_r are distinct odd primes, no one dividing a , then $N = n_1^{m_1} \dots n_r^{m_r}$ divides $a^k - 1$, where $k = \phi(N)/2^{r-1}$.

R. D. Carmichael¹⁰⁹ proved that the maximum indicator of any odd number is even; that of a number, whose least prime factor is of the form $4l+1$, is a multiple of 4; that of $p(2p-1)$ is a multiple of 4 if p and $2p-1$ are odd primes.

A. Cunningham¹¹⁰ gave a table of the values of ν , where $(p-1)/\nu$ is the exponent to which 2 belongs modulo $p^n < 10000$, the omitted values of p being those for which $\nu=1$ or 2 and hence are immediately distinguished by the quadratic character of 2 (extension of his Binary Canon⁹⁵). A list is given of errata in the table by Reuschle.⁴⁵ An announcement is made of the manuscript of tables of the exponents to which 3, 5, 6, 7, 10, 11, 12 belong modulo $p^n < 10000$, and the least positive and negative primitive roots of each prime < 10000 [now in type and extended in manuscript to $p^n < 22000$].

A. Cunningham¹¹¹ defined the sub-Haupt-exponent ξ_1 of a base q to modulus $m = q^{a_0}\eta_0$ (where η_0 is prime to q , and $a_0 \geq 0$) to be the exponent to which q belongs modulo η_0 . Similarly, let ξ_2 be the exponent to which q belongs modulo η_1 , where $\xi_1 = q^{a_1}\eta_1$; etc. Then the ξ 's are the successive sub-Haupt-exponents, and the train ends with $\xi_{r+1} = 1$, corresponding to $\eta_r = 1$. His table I gives these ξ_k for bases $q = 2, 3, 5$ and for various moduli including the primes < 100 .

Paul Epstein¹¹² desired a function $\psi(m)$, called the Haupt-exponent for modulus m , such that $a^{\psi(m)} \equiv 1 \pmod{m}$ for every integer a prime to m and such that this will not hold for an exponent $< \psi(m)$. Thus $\psi(m)$ is merely Cauchy's²⁶ maximum indicator. Although reference is made to Lucas,⁷³ who gave the correct value of $\psi(m)$, Epstein's formula requires modification when $m=4$ or 8 since it then gives $\psi=1$, whereas $\psi=2$. The number $\chi(m, \mu)$ of roots of $x^\mu \equiv 1 \pmod{m}$ is $2d_0d_1 \dots d_n$ if m is divisible by 4 and if μ is odd, but is $d_1 \dots d_n$ in the remaining cases, where, for $m = 2^{a_0}p_1^{a_1} \dots p_n^{a_n}$, d_i is the g. c. d. of μ and $\phi(p_i^{a_i})$, and d_0 the g. c. d. of μ and 2^{a_0-2} , when $a_0 > 1$. The number of integers belonging to the exponent $\mu = p^\alpha q^\beta \dots$ modulo m is

$$\{\chi(m, p^\alpha) - \chi(m, p^{\alpha-1})\} \{\chi(m, q^\beta) - \chi(m, q^{\beta-1})\} \dots$$

¹⁰⁷Revue de Math. (Peano), Turin, 8, 1905, 89-117.

¹⁰⁸Göteborgs Kungl. Vetenskaps-Handlingar, (4), 7-8, 1905, 12-14.

¹⁰⁹Amer. Math. Monthly, 13, 1906, 110.

¹¹⁰Quar. Jour. Math., 37, 1906, 122-145. Manuscript announced in Mess. Math., 33, 1903-4, 145-155 (with list of errata in earlier tables); British Assoc. Report, 1904, 443; l'intermédiaire des math., 16, 1909, 240; 17, 1910, 71. Cf. Cunningham.¹²³

¹¹¹Proc. London Math. Soc., 5, 1907, 237-274.

¹¹²Archiv Math. Phys., (3), 12, 1907, 134-150.

This formula is simplified in the case $\mu = \psi(m)$ and the numbers belonging to this Haupt-exponent are called primitive roots of m . The primitive roots of m divide into families of $\phi(\psi(m))$ each, such that any two of one family are powers of each other modulo m , while no two of different families are powers of each other. Each family is subdivided. In general, not every integer prime to m occurs among the residues modulo m of the powers of the various primitive roots of m .

A. Cunningham¹¹³ considered the exponent ξ to which an odd number q belongs modulo 2^m ; and gave the values of ξ when $m \leq 3$, and when $q = 2^x \Omega \pm 1$ (Ω odd), $m > 3$. When $q = 2^x \mp 1$ and $m > x + 1$, the residue of $q^{\xi/2^j}$ can usually be expressed in one of the forms 1 ∓ 2^a , $1 \mp 2^a \mp 2^b$.

G. Fontené¹¹⁴ determined the numbers N which belong to a given exponent $p^{m-h}\delta$ modulo p^m , where δ is a given divisor of $p-1$, and $h \geq 1$, without employing a primitive root of p^m . If $p > 2$, the conditions are that N shall belong to the exponent δ modulo p and that the highest power of p dividing $N^\delta - 1$ shall be p^h , $1 \leq h \leq m$.

*M. Demeczky¹¹⁵ discussed primitive roots.

E. Landau¹¹⁶ proved the existence of primitive roots of powers of odd primes, discussed systems of indices for any modulus n , and treated the characters of n .

G. A. Miller¹¹⁷ noted that the determination of primitive roots of g corresponds to the problem of finding operators of highest order in the cyclic group G of order g . By use of the group of isomorphisms of G it is shown that the primitive roots of g which belong to an exponent $2q$, where q is an odd prime, are given by $-\alpha^2$, when α ranges over those integers between 1 and $g/2$ which are prime to g . As a corollary, the primitive roots of a prime $2q+1$, where q is an odd prime, are $-\alpha^2$, $1 < \alpha < q+1$.

A. N. Korkine¹¹⁸ gave a table showing for each prime $p < 4000$ a primitive root g and certain characters which serve to solve any solvable congruence $x^q \equiv a \pmod{p}$, where q is a prime dividing $p-1$. Let q^a be the highest power of q dividing $p-1$. The characters of degree q are the solutions of

$$u^q \equiv 1, \quad u'^q \equiv u, \quad u''^q \equiv u', \dots, \quad (u^{(a-1)})^q \equiv u^{(a-2)} \pmod{p}$$

and hence are the residues of the powers of $g^{(p-1)/q^k}$ for $k = 1, \dots, a$. There are noted some errors in the Canon of Jacobi²³ and the table of Burckhardt. Korkine stated that if p is a prime and a belongs to the exponent $e = (p-1)/\delta$, exactly $\phi(p-1)/\phi(e)$ of the roots of $x^\delta \equiv a \pmod{p}$ are primitive roots of p .

K. A. Posse¹¹⁹ remarked that Korkine constructed his table without knowing of the table by Wertheim,⁹¹ and extended Korkine's tables to 10000.

¹¹³Messenger of Math., 37, 1907-8, 162-4.

¹¹⁴Nouv. Ann. Math., (4), 8, 1908, 193-216.

¹¹⁵Math. és Phys. Lapok, Budapest, 17, 1908, 79-86.

¹¹⁶Handbuch...Verteilung der Primzahlen, I, 1909, 391-414, 478-486.

¹¹⁷Amer. Jour. Math., 31, 1909, 42-4.

¹¹⁸Matem. Sborn. Moskva (Math. Soc. Moscow), 27, 1909, 28-115, 120-137 (in Russian). Cf. D. A. Grave, 29, 1913, 7-11. The table was reprinted by Posse.¹²⁸

¹¹⁹Ibid., 116-120, 175-9, 238-257. Reprinted by Posse.¹²⁹

R. D. Carmichael¹²⁰ called a number a primitive λ -root modulo n if it belongs to the exponent $\lambda(n)$, defined in Ch. III, Lucas.¹¹⁰ The existence of primitive λ -roots g is proved. The product of those powers of g which are primitive λ -roots is $\equiv 1 \pmod{n}$ if $\lambda(n) > 2$. A method is given to solve $\lambda(x) = a$, and the solutions tabulated for $a \leq 24$.

C. Posse¹²¹ noted that in Wertheim's^{83, 91} table, the primitive root 14 of 2161 should be replaced by 23, while 10 is not a primitive root of 3851.

E. Maillet¹²² described the manuscript table by Chabanel, deposited in the library of the University of Paris, giving the indices for primes under 10000 and data to determine the number having a given index.

F. Schuh¹²³ showed how to form the congruence for the primitive roots of a prime and gave two further proofs of the existence of primitive roots. He treated binomial congruences, quadratic residues and made applications to periodic fractions to any base. For any modulus n , he found the least m for which $x^m \equiv 1 \pmod{n}$ holds for every x prime to n , and derived the solutions n of $\phi(n) = m$, i. e., n 's having primitive roots.

F. Schuh¹²⁴ discussed the solution of $x^q \equiv 1 \pmod{p^a}$ with the least computation. If x belongs to the exponent q modulo n , the powers of x give a cycle of $\phi(q)$ numbers each with the "period" q . The numbers prime to n and having the period q may form several such cycles—more than one if n has no primitive root and q is the maximum period. If $n = 2^a$ ($a > 2$), then $q = 2^s$ ($s \leq a - 2$) and the number of cycles is 1, 3 or 2 according as $s = 0$, $s = 1$ or $s > 1$. In the last case, the cycles are formed by $2^{a-s}(2k+1) \mp 1$.

When q is even, x is said to be of the first or second kind according as $x^{q/2} \equiv -1 \pmod{n}$ or not. If the numbers of a cycle are of the second kind, we get a new cycle of the second kind by changing the signs of the numbers of the first cycle. While for moduli n having primitive roots there exist no numbers of the second kind, when n has no primitive roots and q is a possible even period, there exist at least two cycles of the second kind and of period q . Finally, there is given a table showing the number of cycles of each kind for moduli ≤ 150 .

M. Kraitchik¹²⁵ gave a table showing for each prime $p < 10000$ a primitive root of p and the least solutions of $2^x \equiv 1$, $10^y \equiv 1 \pmod{p}$.

*J. Schumacher¹²⁶ discussed indices.

L. von Schrutka¹²⁷ noted that, if q, r, \dots are the distinct primes dividing $p-1$, where p is a prime, all non-primitive roots of p satisfy

$$\left(x^{\frac{p-1}{q}} - 1\right)\left(x^{\frac{p-1}{r}} - 1\right) \dots \equiv 0 \pmod{p}.$$

¹²⁰Bull. Amer. Math. Soc., 16, 1909-10, 232-7. Also, Theory of Numbers, pp. 71-4.

¹²¹Acta Math., 33, 1910, 405-6.

¹²²L'intermédiaire des math., 17, 1910, 19-20.

¹²³Supplement de Vriend der Wiskunde, Culemborg, 22, 1910, 34-114, 166-199, 252-9; 25, 1913, 33-59, 143-159, 228-259.

¹²⁴Ibid., 23, 1911, 39-70, 130-159, 230-247.

¹²⁵Sphinx-Oedipe, May, 1911, Numéro Spécial, pp. 1-10; errata listed p. 122 by Cunningham and Woodall. Extension to 25000, 1912, 25-9, 39-42, 52-5; errata, 93-4, by Cunningham.

¹²⁶Blätter Gymnasial-Schulwesen, München, 47, 1911, 217-9.

¹²⁷Monatshefte Math. Phys., 22, 1911, 177-186.

To this congruence he applied Hurwitz's⁴² method (Ch. VIII) of finding the number of roots and concluded that there are $p-1-\phi(p-1)$ roots. Hence there exist $\phi(p-1)$ primitive roots of p .

A. Cunningham and H. J. Woodall¹²⁸ continued to $p < 100000$ the table of Cunningham¹¹⁰ of the maximum residue indices ν of 2 modulo p .

C. Posse¹²⁹ reproduced Korkine's¹¹⁸ and his own¹¹⁹ tables and explained their use in the solution of binomial congruences.

C. Krediet¹³⁰ treated $x^e \equiv 1 \pmod{n}$ of Lucas,¹¹⁰ Ch. III, and called x a primitive root if it belongs to the exponent φ . The powers of such a root are placed at equal intervals on a circle for various n 's.

G. A. Miller¹³¹ proved by use of group theory that, if m is arbitrary, the sum of those integers $< m$ and prime to m which belong to an exponent divisible by 4 is $\equiv 0 \pmod{m}$, and the sum of those belonging to the exponent 2 is $\equiv -1 \pmod{m}$; and proved the corresponding theorem by Stern¹⁵ for a prime modulus.

A. Cunningham¹³² tabulated the number of primes $p < 10^4$ for which y belongs to the same exponent modulo p , for $y = 2, 3, 5, 6, 7, 10, 11, 12$; and the number of primes p in each 10000 to 10^5 for which y ($y = 2$ or 10) belongs to the same exponent modulo p . Also, for the same ranges on p and y , the number of primes p for which $y^k \equiv 1 \pmod{p}$ is solvable, where k is a given divisor of $p-1$.

A. Cunningham¹³³ stated that he had finished the manuscript of a table of Haupt-exponents to bases 3, 5, 6, 7, 11, 12 for all prime powers < 15000 ; also canons giving at sight the residues of z^r modulo $p^k < 10000$ for $z = 2, r \leq 100$; $z = 3, 5, 7, 10, 11, r \leq 30$.

J. Barinaga¹³⁴ considered a number a belonging to the exponent g modulo p , a prime. If a is not divisible by g , the sum of the a th powers of the numbers forming the period of a modulo p is divisible by p . The sum of their products n at a time is congruent to zero modulo p if $n < g$, but to $\neq 1$ if $n = g$, according as g is even or odd.

A. Cunningham¹³⁵ listed errata in his Binary Canon⁹⁵ and Jacobi's Canon.²³

G. A. Miller¹³⁶ employed the group formed by the integers $< m$ and prime to m , combined by multiplication modulo m , to show that, if a number is $\equiv \pm 1 \pmod{2^\gamma}$, but not modulo $2^{\gamma+1}$, where $1 < \gamma < \beta$, it belongs to the exponent $2^{\beta-\gamma}$ modulo 2^β . Also, if p is an odd prime, and $N \equiv 1 \pmod{p}$, N belongs to the exponent $p^{\beta-\gamma}$ modulo p^β if and only if $N-1$ is divisible by p^γ , but not by $p^{\gamma+1}$, where $\beta > \gamma \geq 1$.

¹²⁸Quar. Jour. Math., 42, 1911, 241-250; 44, 1913, 41-48, 237-242; 45, 1914, 114-125.

¹²⁹Acta Math., 35, 1912, 193-231, 233-252.

¹³⁰Wiskundig Tijdschrift, Haarlem, 8, 1912, 177-188; 9, 1912, 14-38; 10, 1913, 40-46, 87-97. (Dutch.)

¹³¹Amer. Math. Monthly, 19, 1912, 41-6.

¹³²Proc. London Math. Soc., (2), 13, 1914, 258-272.

¹³³Messenger Math., 45, 1915, 69. Cf. Cunningham,¹¹⁰

¹³⁴Annaes Sc. Acad. Polyt. do Porto, 10, 1915, 74-6.

¹³⁵Messenger Math., 46, 1916, 57-9, 67-8.

¹³⁶Ibid., 101-3.

A. Cunningham¹³⁷ gave five primes p for which there is a maximum number of exponents to which the various numbers belong modulo p .

On exponents and indices, see Lebesgue¹⁷⁴⁻⁶ and Bouniakowsky¹⁷⁹; also Reuschle⁶⁹ of Ch. VI, Bouniakowsky¹¹¹ of Ch. XIV, and Calvitti⁴⁸ of Ch. XX.

BINOMIAL CONGRUENCES.

Bhāscara Achārya¹⁴⁹ (1150 A. D.) found y such that $y^2 - 30$ is divisible by 7 by solving $y^2 = 7c + 30$. Changing 30 by multiples of 7, we reach a perfect square 16 with the root 4. Hence set

$$7c + 30 = (7n + 4)^2, \quad c = 7n^2 + 8n - 2, \quad y = 7n + 4.$$

Taking $n = 1$, we get $y = 11$. Such a problem is impossible if, after abrading the absolute term (30 above) by the divisor (7 above) and the addition of multiples of the divisor, we do not reach a square.

Similarly for the case of a cube, with corresponding conditions for impossibility (§206, p. 265). For $y^3 = 5e + 6$, abrade 6 by the divisor 5 to get the cube 1; adding 43·5, we get $216 = 6^3$. Hence set $y = 5n + 6$.

An anonymous Japanese manuscript¹⁵⁰ of the first part of the eighteenth century gave a solution of $x^n - ky = a$ by trial. The residues a_1, \dots, a_{k-1} of $1^n, \dots, (k-1)^n$ modulo k are formed; if $a_r = a$, then $x = r$. It was noted that $a_{k-r} = a_r$ or $k - a_r$, according as k is even or odd, and that the residue of r^n is r times that of r^{n-1} .

Matsunaga,^{150a} in the first half of the eighteenth century, solved $a^2 + bx = y^2$ by expressing b as a product mn and finding p, q and A so that $mp - nq = 1$, $2pa \equiv A \pmod{n}$. Then $x = (Am - 2a)A/n$ [and $y = a - mb$]. But if $Am = 2a$, write $A + n$ in place of A and proceed as before. Or write $2a + b$ in the form $bQ + R$, whence $x = 2a + b - (Q + 1)R$. To solve $69 + 11x = y^2$, consider the successive squares until we reach $5^2 \equiv 3 \pmod{11}$. Write $2 \cdot 5 + 11$ in the form $1 \cdot 11 + 10$. Then for $a = 5$, $b = 11$, $Q = 1$, $R = 10$, the preceding expression for x becomes 1, whence $5^2 + 11 \cdot 1 = 6^2$. Then write $2 \cdot 6 + 11$ in the form $2 \cdot 11 + 1$. Then $23 - (2 + 1) \cdot 1 = 20$ gives $6^2 + 20 \cdot 11 = 16^2$, and $x = (256 - 69)/11 = 17$.

L. Euler¹⁵¹ proved that, if n divides $p - 1$, where p is a prime, and if $a = c^n + kp$, then (by powering and using Fermat's theorem), $a^{(p-1)/n} - 1$ is divisible by p . Conversely, if $a^m - 1$ is divisible by the prime $p = mn + 1$, we can find an integer y such that $a - y^n$ is divisible by p . For,

$$a^m - y^{mn} = (a - y^n)Q(y),$$

and the differences of order $mn - n$ of $Q(1), Q(2), \dots, Q(mn)$ are the same

¹³⁷Math. Quest. and Solutions (Ed. Times), 3, 1917, 61-2; corrections, p. 65.

¹⁴⁹Vijja-ganita, §§ 204-5; Algebra, with arith. and mensuration, from the Sanscrit of Brahmagupta and Bhāscara, transl. by H. T. Colebrooke, London, 1817, pp. 263-4.

¹⁵⁰Abhand. Geschichte Math. Wiss., 30, 1912, 237.

^{150a}Ibid., 234-5.

¹⁵¹Novi Comm. Acad. Petrop., 7, 1758-9 (1755), p. 49, seq., §64, §72, §77; Comm. Arith., 1, 270-1, 273. In Novi Comm., 1, 1747-8, p. 20; Comm. Arith., 1, p. 60, he proved the first statement and stated the converse

as those of the term y^{mn-n} for $y=1, \dots, mn$, and hence equal $(mn-n)!$, so that $Q(y)$ is not divisible by p for some values $1, \dots, mn$ of y .

Euler¹⁵² recurred to the subject. The main conclusion here and from his former paper is the criterion that, if $p=mn+1$ is a prime, $x^n \equiv a \pmod{p}$ has exactly n roots or no root, according as $a^m \equiv 1 \pmod{p}$ or not. In particular, there are just m roots of $a^m \equiv 1$, and each root a is a residue of an n th power.

Euler^{152a} stated that, if $aq+b=p^2$, all the values of x making $ax+b$ a square are given by $x=ay^2 \pm 2py+q$.

J. L. Lagrange¹⁵³ gave the criterion of Euler, and noted that if p is a prime $4n+3$, $B^{(p-1)/2} - 1$ is divisible by p , so that $x \equiv B^{n+1}$ is a root of $x^2 \equiv B \pmod{p}$. Given a root ξ of the latter, where now p is any odd prime not dividing B , we can find a root of $x^2 \equiv B \pmod{p^2}$ by setting $x = \xi + \lambda p$, $\xi^2 - B = p\omega$. Then $x^2 - B = (\lambda^2 + \mu)p^2$ if $2\xi\lambda + \omega = \mu p$. The latter can be satisfied by integers λ, μ since 2ξ and p are relatively prime. We can proceed similarly and solve $x^2 \equiv B \pmod{p^n}$.

Next, consider $\xi^2 \equiv B \pmod{2^n}$, for $n > 2$ and B odd (since the case B even reduces to the former). Then $\xi = 2z+1$, $\xi^2 - B = Z+1-B$, where $Z = 4z(z+1)$ is a multiple of 8. Thus $1-B$ must be a multiple of 8. Let $n > 3$ and $1-B = 2^r\beta$, $r > 3$. If $r \geq n$, it suffices to take $z = 2^{n-2}\zeta$, where ζ is arbitrary. If $r < n$, Z must be divisible by 2^r , whence $z = 2^{r-2}\zeta$ or $2^{r-2}\zeta - 1$. Hence $w \equiv \zeta(2^{r-2}\zeta \pm 1) + \beta$ must be divisible by 2^{n-r} . If $n-r \leq r-2$, it suffices to take $\zeta \equiv \beta$ divisible by 2^{n-r} . The latter is a necessary condition if $n-r > r-2$. Thus $\zeta = 2^{r-2}\rho \mp \beta$, $w = 2^{r-2}(\zeta^2 \pm \rho)$. Hence $\zeta^2 \pm \rho$ must be divisible by 2^{n-2r+2} . We have two sub-cases according as the exponent of 2 is \leq or $> r-1$; etc.

Finally, the solution of $x^2 \equiv B \pmod{m}$ reduces to the case of the powers of primes dividing m . For, if f and g are relatively prime and $\xi^2 - B$ is divisible by f , and $\psi^2 - B$ by g , then $x^2 - B$ is divisible by fg if $x = \mu f \pm \xi = \nu g \pm \psi$. But the final equality can be satisfied by integers μ, ν since f is prime to g .

A. M. Legendre¹⁵⁴ proved that if p is a prime and ω is the g. c. d. of n and $p-1 = \omega p'$, there is no integral root of

$$(1) \quad x^n \equiv B \pmod{p}$$

unless $B^{p'} \equiv 1 \pmod{p}$; if the last condition is satisfied, there are ω roots of (1) and they satisfy

$$(2) \quad x^\omega \equiv B^l \pmod{p},$$

where l is the least positive integer for which

$$(3) \quad ln - q(p-1) = \omega.$$

For, from (1) and $x^{p-1} \equiv 1$, we get $x^{ln} \equiv B^l$, $x^{q(p-1)} \equiv 1$, and hence (2), by use of (3). Set $n = \omega n'$. Then, by (2) and (1),

$$B^{n'l} \equiv x^n \equiv B, \quad B^{p'l} \equiv x^{p'\omega} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

¹⁵²Novi Comm. Petrop., 8, 1760-1, 74; Opusc. Anal. 1, 1772, 121; Comm. Arith., 1, 274, 487.

^{152a}Opera postuma, I, 1862, 213-4 (about 1771).

¹⁵³Mém. Acad. R. Sc. Berlin, 23, année 1767, 1769; Oeuvres, 2, 497-504.

¹⁵⁴Mém. Ac. R. Sc. Paris, 1785, 468, 476-481. (Cf. Legendre.¹⁵⁵)

Since $ln' - qp' = 1$, the first gives $B^{qp'} \equiv 1$. Hence

$$B^{p'} = B^{p'(ln' - qp')} = (B^{p'l})^{n'} / (B^{qp'})^{p'} \equiv 1 \pmod{p}.$$

Conversely, if $B^{p'} \equiv 1$,

$$x^{p-1} - 1 \equiv x^{p'\omega} - B^{p'l} \pmod{p}$$

has the factor $x^\omega - B^l$, so that (Lagrange³) congruence (2) has ω roots.

If $4n$ divides $p-1$, the roots of $x^{2n} \equiv -1 \pmod{p}$ are the odd powers of an integer belonging to the exponent $4n$ modulo p .

Let n divide $p-1$, and m divide $(p-1)/n$. Let ω be the g. c. d. of m, n and set $n = \omega\nu$. Determine positive integers l and q such that $lv - qm = 1$. If $B^m \equiv \pm 1 \pmod{p}$, (1) is satisfied by the roots of $x^\omega \equiv B^l y \pmod{p}$, where y ranges over the roots of $y^v \equiv (\pm 1)^q \pmod{p}$. For, the last two congruences give

$$x^n = x^{\nu\omega} \equiv B^{\nu l} y^\nu \equiv B^{qm+1} (\pm 1)^q \equiv B \pmod{p}.$$

Hence by means of the roots of $y^v \equiv \pm 1$, we reduce the solution of (1) to binomial congruences of lower degrees. In particular, let $n=2$, $m=(p-1)/2$, and let 2 be prime to m , so that $p=4a-1$, $l=a$, $q=1$. Then $x^2 \equiv B \pmod{p}$ requires that $B^m \equiv 1$, so that we have the solutions $x \equiv \pm B^a$ without trial (Lagrange¹⁵³). Next, if $n=2$ and $B^{2k+1} \equiv -1$, the theorem gives $x \equiv B^{k+1} y$, where $y^2 \equiv -1$. But we may generalize the last result. Consider $x^2 + c^2 \equiv 0 \pmod{p}$. Since p must have the form $4a+1$, we have $p=f^2+g^2$. Determine u and z so that $c=gu-pz$. Then $x \equiv fu \pmod{p}$.

Let a belong to the exponent nw modulo p , where w divides $(p-1)/n$. Then the roots of $B^w \equiv 1 \pmod{p}$ are $B \equiv a^{\nu\mu}$ ($\mu=1, \dots, w-1$), and, for a fixed B , the roots of (1) are $x = a^{mw+\mu}$ ($m=0, 1, \dots, n-1$). For, a^n belongs to the exponent w , whence $B \equiv a^{\nu\mu}$.

Legendre¹⁵⁵ gave the same theorems in his text. He added that, knowing a root θ of (1), it is easy to find a root of $x^n \equiv B \pmod{p^a}$, with the possible exception of the case in which n is divisible by p . Let $\theta^n - B = Mp$ and set $x = \theta + Ap$. Then $x^n - B$ is divisible by p^2 if

$$M + n\theta^{n-1}A = pM',$$

which can be satisfied by integers A, M' if n is not divisible by p . To solve (1) when p is composite, $p = a^\alpha b^\beta \dots$, where a, b, \dots are distinct primes, determine all the roots λ of $\lambda^n \equiv B \pmod{a^\alpha}$, all the roots μ of $\mu^n \equiv B \pmod{b^\beta}, \dots$. Then if $x \equiv \lambda \pmod{a^\alpha}$, $x \equiv \mu \pmod{b^\beta}, \dots$, x will range over all the roots of (1).

Legendre¹⁵⁶ noted that if p is a prime $8n+5$ we can give explicitly the solutions of $x^2 + a \equiv 0 \pmod{p}$ when it is solvable, viz., when $a^{4n+2} \equiv 1$. For, either $a^{2n+1} + 1 \equiv 0$ and $x = a^{n+1}$ is a solution, or $a^{2n+1} - 1 \equiv 0$ and $\theta = a^{n+1}$ satisfies $\theta^2 - a \equiv 0 \pmod{p}$, so that it remains only to solve $x^2 + \theta^2 \equiv 0$, which was done at the end of his¹⁵⁴ memoir. For $p=8n+1$, let $n=a\beta$, where a is a power of 2 and β is odd; if $a^\beta \equiv \pm 1$, $x^2 + a \equiv 0$ can be solved as in the

¹⁵⁵Théorie des nombres, 1798, 411-8; ed. 2, 1808, 349-357; ed. 3, 1830, Nos. 339-351; German transl. by Maser, 1893, 2, pp. 15-22.

¹⁵⁶Ibid., 231-8; ed. 2, 1808, pp. 211-219; Maser, I, pp. 246-7.

case $p=8n+5$; but in general no such direct solution is known, and it is best to represent some multiple of p by the form y^2+az^2 .

If we have found θ such that θ^2+a is divisible by the prime p , not dividing a , we readily solve $x^2+a\equiv 0 \pmod{p^n}$. For, from

$$(\theta \pm \sqrt{-a})^n = r \pm s\sqrt{-a}, \quad (\theta^2+a)^n = r^2+as^2,$$

r^2+as^2 is divisible by p^n . Now s is not divisible by p . Thus we may take $r=sp+p^ny$, whence x^2+a is divisible by p^n . [Cf. Tchebychef, *Theorie der Congruenzen*, §30.]

The case of any composite modulus N is easily reduced to the preceding (end of Lagrange's¹⁵³ paper). Legendre proved that, if N is odd and prime to a , the number of solutions of $x^2+a\equiv 0 \pmod{N}$ is 2^{i-1} where i is the number of distinct prime factors of N ; the same is true for modulus $2N$. Henceforth let N be odd or the double of an odd number and let d be the g. c. d. of N and a . If d has no square factor, the congruence has 2^{i-1} roots, where i is the number of distinct odd prime factors of N not dividing a . But if $d=\omega\psi^2$, where ω has no square factor, the congruence has $2^{i-1}\psi$ roots where i is the number of distinct odd prime factors of N/d .

C. F. Gauss¹⁵⁷ treated congruence (1) by the use of indices. However, we can give a direct solution (arts. 66-68) when a root is known to be congruent to a power of B . For, by (1) and $x\equiv B^k$, $B\equiv B^{kn}$. If therefore a relation of the last type is known, a root of (1) is B^k . The condition for the relation is $1\equiv kn \pmod{t}$, where t is the exponent to which B belongs modulo p . It is shown that t must divide $m=(p-1)/n$. We may discard from m any factor of n ; if the resulting number is m/q , the unique solution k of $1\equiv kn \pmod{m/q}$ is the desired k . [Cf. Poinsot¹⁶⁵.]

Gauss (arts. 101-5) gave the usual method of reducing the solution of $x^2\equiv A \pmod{m}$ for any composite modulus to the case of a prime modulus and gave the number of roots modulo p^n in the various possible subcases. His well-known and practical "method of exclusion" (arts. 319-322) employs successive small powers of primes as moduli. Another method (arts. 327-8) is based on the theory of binary quadratic forms [cf. Smith¹⁷⁰].

The congruence $ax^2+bx+c\equiv 0 \pmod{m}$ is reduced (art. 152) to $y^2\equiv b^2-4ac \pmod{4am}$. For each root y , it remains to solve $2ax+b\equiv y \pmod{4am}$.

Gauss¹⁵⁸ showed in a somewhat incomplete posthumous paper that, if t is a prime and $t^{n-1}(t-1)=a^\alpha b^\beta \dots$, where a, b, \dots are distinct primes, the solution of $x^n\equiv 1 \pmod{t^n}$ may be made to depend upon the solution of α congruences of degree a , β congruences of degree b , etc. Use is made of the periods formed of the primitive roots of the congruence, as in Gauss' theory of roots of unity.

Legendre¹⁵⁹ solved $x^2+a\equiv 0 \pmod{2^m}$ when a is of the form $-1\mp 8a$ by

¹⁵⁷Disquis. Arith., 1801, Arts. 60-65.

¹⁵⁸Werke, 2, 1863, 199-211. Maser's German transl. of Gauss' Disq. Arith., etc., 1889, 589-601 (comments, p. 683).

¹⁵⁹Théorie des nombres, ed. 2, 1808, pp. 358-60 (Nos. 350-2). Maser, 2, 1893, 25-7.

use of the expansion of $(1+z)^{1/2}$:

$$\sqrt{1 \pm 8a} = 1 \pm \frac{1}{2}2^3a - \frac{1 \cdot 1}{2 \cdot 4}2^6a^2 \pm \frac{1 \cdot 1 \cdot 3}{2 \cdot 4 \cdot 6}2^9a^3 - \dots \pm N2^{3n}a^n + \dots,$$

$$N = \frac{1 \cdot 1 \cdot 3 \cdot 5 \dots (2n-3)}{2 \cdot 4 \cdot 6 \cdot 8 \dots 2n}.$$

The coefficient of a^n is an integer divisible by 2^{n+1} . Retain only the terms whose coefficients are not divisible by 2^{m-1} and call their sum θ . Hence every term of $\theta^2 + a$ is divisible by 2^m . Thus the general solution of the proposed congruence is $x \equiv 2^{m-1}x' \pm \theta$.

P. S. Laplace¹⁶⁰ attempted to prove that, if p is a prime and $p-1=ae$, there exists an integer $x < e$ such that $x^e - 1$ is not divisible by p . For, if $x=e$ and all earlier values of x make $x^e - 1$ divisible by p ,

$$f \equiv (e^e - 1) - e \{ (e-1)^e - 1 \} + \binom{e}{2} \{ (e-2)^e - 1 \} - \dots$$

would be divisible by p . The sum of the second terms of the binomials is

$$-1 + e - \binom{e}{2} + \dots = -(1-1)^e = 0,$$

while the sum of the first terms of the binomials is $e!$ by the theory of differences, and is not divisible by p since $e < p$. [But the former equality implies that the last term of f is $(-1)^e(0-1)$, whereas the theorem is trivial if x is allowed to take the value 0. Again, nothing in the proof given prevents a from being unity; then the statement that there is a positive integer $x < p-1$ such that $x^{p-1} - 1$ is not divisible by p contradicts Fermat's theorem.]

L. Poincot¹¹ deduced roots of $x^n \equiv 1 \pmod{p}$ from roots of unity.

M. A. Stern¹⁵ (p. 152) proved that if n is odd and p is a prime, $x^n \equiv -1 \pmod{p}$ is solvable and the number of roots is the g. c. d. of n and $p-1$; while, if n is even, it is solvable if and only if the factor 2 occurs in $p-1$ to a higher power than in n .

G. Libri¹⁶¹ gave a long formula, involving sums of trigonometric functions, for the number of roots of $x^2 + c \equiv 0 \pmod{p}$.

V. A. Lebesgue¹³ applied a theorem on $f(x_1, \dots, x_k) \equiv 0$ to derive Legendre's¹⁵⁴ condition $B' \equiv 1$ for the existence of roots of (1), and the number of roots. Cf. Lebesgue¹⁷ of Ch. VIII.

Erlerus²⁵ (pp. 9-13) proved that, if p_1, \dots, p_μ are distinct odd primes,

$$x^2 \equiv 1 \pmod{2^\nu p_1^{e_1} \dots p_\mu^{e_\mu}}$$

has 2^μ , 2^μ , $2^{\mu+1}$ or $2^{\mu+2}$ roots according as $\nu=0, 1, 2$ or >2 .

For the last result and the like number of roots of $x^2 \equiv a$, see the reports, in Ch. III on Fermat's theorem, of the papers by Brenneke⁵⁷ and Crelle⁵⁸ of 1839, Crelle,⁶⁶ Poincot⁶⁷ (erroneous) and Prouhet⁶⁹ of 1845, and Schering¹⁰² of 1882.

C. F. Arndt¹⁶² proved that the number of roots of $x' \equiv 1 \pmod{p^n}$ for

¹⁶⁰Communication to Lacroix, *Traité Calcul Diff. Int.*, ed. 2, vol. III, 1818, 723.

¹⁶¹*Jour. für Math.*, 9, 1832, 175-7. See Libri,¹⁸ Ch. VIII.

¹⁶²*Archiv Math. Phys.*, 2, 1842, 10-14, 21-22.

p an odd prime is the g. c. d. of t and $\phi(p^n)$; the same holds for modulus $2p^n$. He found the number of roots of $x^2 \equiv r \pmod{m}$, m arbitrary. By using $\Sigma \phi(t) = \delta$, if t ranges over the divisors of δ , he proved (pp. 25–26) the known result that the number of roots of $x^n \equiv 1 \pmod{p}$ is the g. c. d. of n and $p-1$. The product of the roots of the latter is congruent to $(-1)^{\delta+1}$; the sum of the roots is divisible by p ; the sum of the squares of the roots is divisible by p if $\delta > 2$.

P. F. Arndt¹⁶³ used indices to find the number of roots of $x^3 \equiv a$.

A. L. Crelle¹⁶⁴ gave an exposition of known results on binomial congruences.

L. Poinso¹⁶⁵ considered the direct solution of $x^n \equiv A \pmod{p}$, where p is a prime and n is a divisor of $p-1 = nm$ (to which the contrary case reduces). Let the necessary condition $A^m \equiv 1$ be satisfied. Hence we may replace A by A^{1+mk} and obtain the root $x \equiv A^e$ if $1+mk = ne$ is solvable for integers k, e , which is the case if m and n are relatively prime [cf. Gauss¹⁵⁷]. The fact that we obtain a single root $x \equiv A^e$ is explained by the remark that it is a root common to $x^n \equiv A$ and $x^m \equiv 1$, which have a single common root when n is prime to m . Next, let n and m be not relatively prime. Then there is no root A^e if A belongs to the exponent m modulo p . But if A belongs to a smaller exponent m' and if m' is prime to n , there exists as before a root $A^{e'}$, where $1+m'k = ne'$. The number of roots of $x^n \equiv 1 \pmod{N}$ is found (pp. 87–101).

C. F. Arndt¹⁶⁶ proved that $x^t \equiv 1 \pmod{2^n}$, $n > 2$, has the single root 1 if t is odd; while for t even the number of roots is double the g. c. d. of t and 2^{n-2} . The sum of the k th powers of the roots of $x^t \equiv 1 \pmod{p}$ is divisible by the prime p if k is not a multiple of t . By means of Newton's identities it is shown that the sum, sum of products by twos, threes, etc., of the roots of $x^t \equiv 1 \pmod{p}$ is divisible by the prime p , while their product is $\equiv +1$ or -1 according as the number of roots is odd or even. If the sum, sum of products by twos, threes, etc., of m integers is divisible by the prime p , while their product is $\equiv -(-1)^m$, the m integers are the roots of $x^m \equiv 1 \pmod{p}$.

A. Cauchy¹⁶⁷ stated that if $I = p^\lambda q^\mu \dots$, where p, q, \dots are m distinct primes, and if n is an odd prime, $x^n \equiv 1 \pmod{I}$ has n^m distinct roots, including primitive roots, i. e., numbers belonging to the exponent n . [But $x^3 \equiv 1 \pmod{5}$ has a single root.]

Cauchy¹⁶⁸ later restricted p, q, \dots to be primes $\equiv 1 \pmod{n}$. Then $x^n \equiv 1 \pmod{p^\lambda}$ has a primitive root r_1 , and $x^n \equiv 1 \pmod{q^\mu}$ has a primitive root r_2 , so that $x^n \equiv 1 \pmod{I}$ has a primitive root, viz., an integer $\equiv r_1 \pmod{p^\lambda}$ and $\equiv r_2 \pmod{q^\mu}$, etc.; but no primitive root if p, q, \dots are not all $\equiv 1 \pmod{n}$.

¹⁶³Von den Kubischen Resten, Torgau, 1842, 12 pp.

¹⁶⁴Jour. für Math., 28, 1844, 111–154.

¹⁶⁵Jour. de Mathématiques, (1), 10, 1845, 77–87.

¹⁶⁶Archiv Math. Phys., 6, 1845, 380, 396–9.

¹⁶⁷Comptes Rendus Paris, 24, 1847, 996; Oeuvres, (1), 10, 299.

¹⁶⁸Comptes Rendus Paris, 25, 1847, 37; Oeuvres, (1), 10, 331.

Hoëné Wronski¹⁶⁹ stated without proof that, if $x^m \equiv a \pmod{M}$,

$$a = (-1)^{\omega+1} \{hK + (-1)^{k+1} \}^m A[M/K, \omega]^{\omega-2} + Mi, \\ x = h + (-1)^{\pi+k} A[M/K, \pi]^{\pi-1} + Mj,$$

and that M must be a factor of $aK^m - \{hK - (-1)^{k+1} \}^m$. Here the "alephs" $A[M/K, \omega]^r$, for $r=0, 1, \dots$, are the numerators of the reduced fractions obtained in the development of M/K as a continued fraction. In place of K , Wronski wrote the square of $1^{k/1} = k!$. Concerning these formulas, see Hanegraeff,¹⁷¹ Bukaty,¹⁸⁰ Dickstein.¹⁹⁴ Cf. Wronski¹⁵¹ of Ch. VIII.

E. Desmarest³⁷ noted that, if $x^2 + D \equiv 0 \pmod{p}$ is solvable, $x^2 + Dy^2 = mp$ can be satisfied by a value of $m < 3 + p/16$ and a value of $y \leq 3$. His proof is not satisfactory.

D. A. da Silva⁴² (Alasia, p. 31) noted that $x^D \equiv 1 \pmod{m}$, where $m = p_1^{e_1} p_2^{e_2} \dots$, has the roots $\Sigma x_i q_i m / p_i^{e_i}$ where x_i is a root of $x^{D_i} \equiv 1 \pmod{p_i^{e_i}}$, D_i being the g. c. d. of D and $\phi(p_i^{e_i})$, while the q_i 's are integers such that $\Sigma q_i m / p_i^{e_i} \equiv 1 \pmod{m}$.

Da Silva^{169a} proved that a solvable congruence $x^n \equiv r \pmod{m}$ can be reduced to the case r prime to m and then to the case $m = p^a$, p a prime > 2 . Then, if δ is the g. c. d. of n and $\phi(p^a) = \delta \delta_1$, there is a root if and only if $r^{\delta_1} \equiv 1 \pmod{p^a}$ and hence if and only if $r^d \equiv 1 \pmod{p^{a'+1}}$, where $p^{a'}$ is the g. c. d. of n and p^{a-1} , while d is the quotient of $p-1$ by its g. c. d. with n .

H. J. S. Smith¹⁷⁰ indicated a simplification in Gauss'¹⁵⁷ second method of solving $x^2 \equiv A$. If $r^2 + D \equiv 0 \pmod{P}$ is solvable, $mP = x^2 + Dy^2$ is solvable for some value of $m < 2\sqrt{D/3}$. Employing all values of m under that limit for which also

$$\left(\frac{m}{D}\right) = \left(\frac{P}{D}\right),$$

and finding with Gauss all prime representations of the resulting products by the form $x^2 + Dy^2$, we get $\pm r \equiv x'/y'$, x''/y'' , $\dots \pmod{P}$, where x' , y' ; x'' , y'' ; \dots denote the sets of solutions of $mP = x^2 + Dy^2$.

Eg. Hanegraeff¹⁷¹ reduced $x^m \equiv r$ to $\theta^m r \equiv 1 \pmod{p}$ by use of $\theta x \equiv 1$. When p/θ is developed into a continued fraction, let μ and $P_{\mu-1}$ be the number of quotients and number of convergents preceding the last. Let ν , $P_{\nu-1}$ be the corresponding numbers for p/θ^m . Then

$$x \equiv (-1)^{\mu-1} P_{\mu-1}, \quad r \equiv (-1)^{\nu-1} P_{\nu-1} \pmod{p}.$$

For p a prime, we get all roots by taking $\theta = 1, \dots, (p-1)/2$. By starting with $\theta(x-h) \equiv 1$ in place of $\theta x \equiv 1$, we get

¹⁶⁹Réforme des Mathématiques, being Vol. 1 of Réforme du savoir humain, 1847. Wronski's mathematical discoveries have been discussed by S. Dickstein, *Bibliotheca Math.*, (2), 6, 1892, 48-52, 85-90; 7, 1893, 9-14 [on analysis, (2), 8, 1894, 49, 85; (2), 10, 1896, 5]. *Bull. Int. Ac. Sc. Cracovie*, 1896; *Rozprawy*, Krakow, 4, 1913, 73, 396. Cf. *l'intermédiaire des math.*, 22, 1915, 68; 23, 1916, 113, 164-7, 181-3, 199, 231-4; 25, 1918, 55-7.

^{169a}C. Alasia, *Annaes Sc. Acad. Polyt. do Porto*, 9, 1914, 65-95. There are many confusing misprints; for example, five at the top of p. 76.

¹⁷⁰British Assoc. Report, 1860, 120-, §68; *Coll. M. Papers*, 1, 148-9.

¹⁷¹Note sur l'équation de congruence $x^m \equiv r \pmod{p}$, Paris, 1860.

$$x-h \equiv (-1)^{\mu-1} P_{\mu-1}, \quad r \equiv (-1)^{\nu-1} (\theta h + 1)^m P_{\nu-1} \pmod{p}.$$

By taking $\theta = (1^{k/1})^2$ and replacing 1 by $(-1)^{k+1}$ in $\theta(x-h) \equiv 1$, the last results become the fundamental formula given without proof by Wronski¹⁶⁹ in his *Réforme des Mathématiques*.

G. L. Dirichlet¹⁷² discussed the solution of $x^2 \equiv D$ for any modulus.

G. F. Meyer¹⁷³ gave an elementary discussion of the solution of $x^3 \equiv b \pmod{k}$, for k a prime, power of prime, or any integer.

V. A. Lebesgue¹⁷⁴ employed a prime p , a divisor n of $p-1 = nn'$, and a number a belonging to the exponent n' modulo p . Then the roots of $x^n \equiv a \pmod{p}$ are $a^{\alpha} b^{\beta}$, where b is not in the period of a , and b is a quadratic non-residue of p if a is a quadratic residue, and b^n is the least power of b congruent to a term of the period of a . If we set $b^n \equiv a^{\nu} \pmod{p}$, then must $n\alpha + \nu\beta \equiv 1 \pmod{n'}$. The roots x are primitive roots of p . In the construction of a table of indices, his method is to seek a primitive root giving to ± 2 the minimum index (rather than to ± 10 , used by Jacobi); thus we use the theorem for $a = \pm 2$.

Lebesgue¹⁷⁵ gave reasons why the conditions imposed on b in his preceding paper are necessary. He added that when we have found that $x^n \equiv a \pmod{p}$ leads to a primitive root $x = g$ of p , it is easy to solve $x^m \equiv r \pmod{p}$ when m divides $p-1$, by expressing r as a power of g by the equivalent of an abridged table of indices.

Lebesgue¹⁷⁶ noted that the usual method of solution by indices leads to the theorem: If a belongs to the exponent e modulo p , and if n divides $p-1$, and we set $n = e'm$, where e' has only prime factors which divide e , while m is prime to e , then, for every divisor M of m , $x^n \equiv a \pmod{p}$ has $e'\phi(M)$ roots belonging to the exponent M .

If a belongs to the exponent e modulo p , there are $e\phi(n)$ numbers b , not in the period of a , for which $b^n \equiv a^i \pmod{p}$, with n a minimum. A common divisor of n and i does not divide e . Then the n roots of $x^n \equiv a \pmod{p}$ are $a^{\alpha} b^{\beta}$, where $nt - iu - 1 = ev$, $t < e$, $u < n$. This generalization of his¹⁷⁴ earlier theorem is used to find the period of a primitive root of p from the period of 2.

R. Gorgas¹⁷⁷ stated that, if ρ is the residue modulo M of the p th term of $\{(M-1)/2\}^2, \dots, 2^2, 1^2$, then $p(p-1) = \rho \pm m + Ma$, according as $M = 4m \pm 1$. Take the lower signs and solve for p ; we get

$$2p = 1 \pm b, \quad b^2 = M(4a-1) + 4\rho.$$

Set $4\rho = Mc + \rho'$. Hence the initial equation $x^2 = My + \rho$ has been replaced by $b^2 = M(4a + c - 1) + \rho'$ of like form. Let ρ' be the p' th place from the end. The process may be repeated until we reach an equation $P(P-1) = MA + \rho_m - m$ solvable by inspection.

¹⁷²Zahlentheorie, 1863, §§32-7; ed. 2, 1871; ed. 3, 1879; ed. 4, 1894.

¹⁷³Archiv Math. Phys., 43, 1865, 413-36.

¹⁷⁴Comptes Rendus Paris, 61, 1865, 1041-4.

¹⁷⁵Ibid., 62, 1866, 20-23.

¹⁷⁶Ibid., 63, 1866, 1100-3.

¹⁷⁷Ueber Lösung dioph. Gl. 2. Gr., Progr., Magdeburg, 1867.

Ladrasch¹⁷⁸ obtained known results on $x^3 \equiv a$ for any modulus.

V. Bouniakowsky¹⁷⁹ gave a method of solving $q \cdot 3^x \equiv \pm r \pmod{P}$, where P is odd. His first illustration is $3^x \equiv \pm 1 \pmod{25}$. Write the integers $\leq (25-1)/2$ in a line. Under the first four write in order the integers $\equiv 0 \pmod{3}$; under the next four write in reverse order those $\equiv 1$; under the last four write in order those $\equiv 2$.

1*	2*	3*	4*	5	6*	7*	8*	9*	10	11*	12*
3	6	9	12	10	7	4	1	2	5	8	11

Mark with an asterisk 1 in the first line; below it lies 3; mark with an asterisk 3 in the first line; etc. The number 10 of the integers marked with an asterisk is the least solution x of $3^x \equiv -1 \pmod{25}$. The sign is determined by the number of integers in the second set marked by an asterisk. The method applies to any $P=6n+1$. But for $P=6n+5$, we use for the second set of numbers in the second line those $\equiv 2 \pmod{3}$ in reverse order, and for the third set those $\equiv 1$ in order. If $P=23$, we see that each of the 11 numbers in the first line are marked with an asterisk, whence $3^{11} \equiv -1 \pmod{23}$. A like marking occurs for $P=5, 11, 17, 29$. For $P=35$, 12 numbers are marked, whence 12 is the least x for which $3^x \equiv 1 \pmod{35}$. Starting with the unmarked number 5, we get the cycle 5, 15, 10, whence $3^3 \equiv -1 \pmod{7}$; similarly, the cycle 7, 14 gives $3^2 \equiv -1 \pmod{5}$.

For $q \cdot 3^x \equiv \pm 4 \pmod{25}$, we begin with 4 in the second row. Since it lies below 7, we mark 7 with an asterisk in the second row; etc. We use an affix n on the number which is the n th marked by an asterisk.

1	2	3	4	5	6	7	8	9	10	11	12
3*6	6*3	9*5	12*10	10	7*2	4*1	1*7	2*4	5	8*8	11*9

For $q=11$, we have the entry 8^{*8} below 11; hence $11 \cdot 3^8 \equiv -4$, the sign following from the number of entries ≤ 8 in the second set which are marked with an asterisk. Similarly for any $q \leq 12$, except $q=5, 10$.

Bukaty¹⁸⁰ discussed the formula of Wronski.¹⁶⁹

T. N. Thiele¹⁸¹ used a mosaic (empty and filled squares on cross-section paper) to test $y^2 \equiv d \pmod{c}$, where c is an integer or Gauss complex integer $a+b\sqrt{-1}$, employing the graph of $y^2 - cx = d$.

Dittmar¹⁸² discussed $x^3 \equiv r \pmod{p}$. Using Cauchy's¹⁴ explicit congruence for the numbers belonging to a given exponent, he gave the expanded form of the congruence with the roots belonging to the successive exponents 1, ..., 21.

¹⁷⁸Von den Kubischen Resten u. Nichtresten, Progr., Dortmund, 1870.

¹⁷⁹Bull. Ac. Sc. St. Pétersbourg, 14, 1870, 356-375.

¹⁸⁰Déduction et démonstration de trois lois primordiales de la congruence des nombres, Paris, 1873.

¹⁸¹"Om Talmonstre," Forhandl. Skandinaviske Naturforskere, Kjøbenhavn, 11, 1873, 192-5.

¹⁸²Die Theorie der Reste, insbesondere derer vom 3. Grade, nebst einer Tafel der Kubischen Reste aller Primzahlen der Form $6n+1$ zwischen den Grenzen 1 und 100. Progr. Köln Gym., Berlin, 1873.

L. Sancery⁶¹ (pp. 17-23) employed the modulus $M = p^r$ or $2p^r$, where p is an odd prime. Let a belong to the exponent n modulo M . Let Δ be the g. c. d. of m and $\phi(M)/n$. Set $\Delta = \Delta_1 \Delta_2$ where $\Delta_1 = p_1^{e_1} p_2^{e_2} \dots$, and p_i is a prime dividing both Δ and n , and $p_i^{e_i}$ is the power of p_i dividing Δ . Let δ be any divisor of Δ_2 . Then $x^m \equiv a \pmod{M}$ has $\phi(n\Delta_1\delta)/\phi(n)$ roots belonging to the exponent $n\Delta_1\delta$; the power $a\Delta_1\delta$ of such a root is congruent to a , where a can be found by means of a linear congruence. Given a number belonging to the exponent $n\Delta_1\delta$, we can find $\Delta_1\delta$ roots of the congruence.

C. G. Reuschle^{182a} tabulated the roots of $f \equiv 0 \pmod{p}$, where $p = m\lambda + 1$ and λ are primes and f is the maximum irreducible algebraic prime factor of $a^\lambda - 1$; also the roots of

$$\eta^2 + c \equiv 0, \quad \eta^4 + c^2 \equiv 0, \quad \eta^8 + c^4 \equiv 0, \quad \eta^2 \pm \eta + d \equiv 0,$$

for $c < 13$, $d = -1$ to -26 , $d = +2$ to $+21$, and for various cubic and quartic congruences.

A. Kunerth's method for $y^2 \equiv c \pmod{b}$ will be given in Vol. 2, Ch. XII.

E. Lucas^{182b} treated $x^2 + 1 \equiv 0 \pmod{p^m}$, where p is a prime > 2 , for use in the question of the number of satins. Given $a^2 + 1 \equiv 0 \pmod{p}$, set

$$(a + i)^m = A + Bi, \quad \beta B \equiv 1 \pmod{p^m}.$$

Then $A\beta$ is a root x of the proposed congruence.

B. Stankewitsch¹⁸³ proved that if $x^2 \equiv q \pmod{p}$ is solvable, p being an odd prime, the positive root $< p/2$ is $\equiv B/A \pmod{p}$, where

$$A = S_{i-1} + qS_{i-3} + q^2S_{i-5} + \dots + q^{\frac{i-2}{2}}S_1, \quad B = S_i + qS_{i-2} + \dots + q^{\frac{i}{2}},$$

where $i = (p-1)/2$ and S_k denotes the sum of the products of $1, 2, \dots, i$ taken k at a time. Let n be a divisor of $p-1$. Let $F(x)$ be the g. c. d. modulo p of $x^n - 1$ and $\Pi(x^{n/a} - 1)$, where a ranges over the distinct prime factors of n . Call $f(x)$ the quotient of $x^n - 1$ by $F(x)$. Then the roots of $f(x) \equiv 0 \pmod{p}$ are the primitive roots of $x^n \equiv 1 \pmod{p}$. [Cf. Cauchy.¹⁴]

N. V. Bougaief¹⁸⁴ noted that if $p = 8n + 5$ is a prime and if $x^2 \equiv q \pmod{p}$ is solvable, it has the root $q^{(p+3)/8}$ or $(\frac{p-1}{2})! q^{(p+3)/8}$ according as $q^{2n+1} \equiv 1$ or -1 . If $p = 2^l + 1$, l odd, and $q^l \equiv 1$, it has the root $x \equiv q^{(l+1)/2}$. [Legendre.¹⁵⁶]

T. Pepin¹⁸⁵ treated $x^3 \equiv 2$ by tables of indices.

P. Gazzaniga¹⁸⁶ gave a generalization of Gauss' lemma (the case $n = \delta = 2$,

^{182a} Tafeln Complexer Primzahlen. . . , Berlin, 1875. Errata, Cunningham.¹³⁵

^{182b} Géométrie des tissus, Assoc. franç., 40, 1911, 83-6; French transl. of his Italian paper in l'Ingegnere Civile, 1880, Turin.

¹⁸³ Moscow Math. Soc., 10, 1882-3, I, 112 (in Russian).

¹⁸⁴ *Ibid.*, p. 103.

¹⁸⁵ Atti Accad. Pont. Nuovi Lincei, 38, 1884-5, 201.

¹⁸⁶ Atti Reale Istituto Veneto, (6), 4, 1885-6, 1271-9.

$\nu=0$). Separate the residues modulo p of kq , for $k=1, 2, \dots, (p-1)/\delta$, into three sets:

$$0 < r_1, \dots, r_\rho < \frac{p}{\delta} < s_1, \dots, s_\nu < \frac{\delta-1}{\delta} p < t_1, \dots, t_\mu < p$$

and form the differences $m_i = p - t_i$. From the set $1, \dots, (p-1)/\delta$, delete the r_i and m_i ; there remain ν numbers v_i . If y_i is a root of $s_i y_i \equiv v_i \pmod{p}$, then $x^n \equiv q \pmod{p}$ is solvable if and only if $(-1)^\mu y_1 \dots y_\nu \equiv 1 \pmod{p}$, where δ is the g. c. d. of n and $p-1$.

P. Seelhoff¹⁸⁷ gave the known cases in which $x^2 \equiv r \pmod{p}$ can be solved explicitly [Lagrange,¹⁵³ Legendre¹⁵⁶]. In the remaining cases, one uses Gauss' method of exclusion, the process of Desmarest,³⁷ or, with Seelhoff, use various quadratic residues of p (*ibid.*, p. 306). Here $x^2 \equiv 41 \pmod{120097}$ is treated.

A. Berger¹⁸⁸ considered a quadratic congruence reducible to $x^2 \equiv D \pmod{4n}$, where $D \equiv 0$ or $1 \pmod{4}$. If D is prime to n , the number of roots is

$$\psi(D, 4n) = 2\Pi \left\{ 1 + \left(\frac{D}{p} \right) \right\} = 2\Sigma \left(\frac{D}{d} \right) \zeta_d = 2\Sigma \left(\frac{D}{d} \right) \zeta_{d_1},$$

where p ranges over the distinct prime factors of n , while d and d_1 range over the pairs of complementary divisors of n , and $\zeta_d = 0$ or 1 according as d has a square factor or not. If $g(nm) = g(n)g(m)$ for all integers n, m , and $g(1) = 1$,

$$\Sigma \left(\frac{D^2}{n} \right) \psi(D, 4n) g(n) = 2\Sigma \left(\frac{D^2}{n} \right) g(n) \cdot \Sigma \left(\frac{D}{n} \right) g(n) \div \Sigma \left(\frac{D^2}{n} \right) g(n)^2,$$

where n ranges over all positive integers. Mean values are found:

$$\begin{aligned} \sum_{k=1}^n \left(\frac{D^2}{k} \right) \psi(D, 4k) &= \frac{12n}{\pi^2 \Pi(1+1/p)} \sum_{h=1}^{\infty} \left(\frac{D}{h} \right) \frac{1}{h} + \lambda n^{2/3}, \\ \sum_{k=1}^n \psi(\Delta, 4k) &= \frac{12n}{\pi^2} \sum_{h=1}^{\infty} \left(\frac{\Delta}{h} \right) \frac{1}{h} + \lambda_1 n^{2/3}, \end{aligned}$$

where Δ is a fundamental discriminant according to Kronecker, λ, λ_1 are finite for all n 's, and p ranges over all primes.

G. Wertheim¹⁸⁹ presented the theory of $x^2 \equiv a \pmod{m}$.

R. Marcolongo¹⁹⁰ treated $x^2 + P \equiv 0 \pmod{p}$ in the usual manner when explicit solutions are known. Next, from a particular set of solutions x, y of $x^2 + p^m y + P = 0$, where p is a prime > 2 , we get the solution

$$\pm x_1 \equiv x - p^m y [a_1 \dots a_{n-1}] \pmod{p^{m+1}}$$

of $x_1^2 + p^{m+1} y_1 + P = 0$, where $[a_1 \dots a_{n-1}]$ is the numerator of next to the last convergent to the continued fraction for $p^m/(2x)$. The method is Serret's, Alg. Supér., II. For $p=2$ the results obtained are the same as in Dirichlet's Zahlentheorie, §36.

¹⁸⁷Zeitschrift Math. Phys., 31, 1886, 378-80.

¹⁸⁸Öfversigt K. Vetenskaps-Ak. Förhandlingar, Stockholm, 44, 1887, 127-153. Nova Acta regiae soc. sc. Upsalensis, (3), 12, 1884.

¹⁸⁹Elemente der Zahlentheorie, 1887, 182-3, 207-217. ¹⁹⁰Giornale di Mat., 25, 1887, 161-173.

F. J. Studnička¹⁹¹ treated at length the solution in integers x, y ($y < b$) of $bx+1=y^2$, discussed by Leibniz in 1716.

L. Gegenbauer¹⁹² gave a new derivation of the equations of Berger¹⁸⁸ leading to asymptotic expressions for the number of solutions of $x^2 \equiv D$.

A. Tonelli¹⁹³ gave a method of solving $x^2 \equiv c \pmod{p}$, when p is a prime $4h+1$ and some quadratic non-residue g of p is known. Set $p=2^s\gamma+1$, where γ is odd. By Euler's criterion, the power $\gamma 2^{s-1}$ of c and g are congruent to $+1, -1$. Set $\epsilon_0=0$ or 1 , according as the power $\gamma 2^{s-2}$ of c is congruent to $+1$ or -1 . Then

$$g^{\epsilon_0 \gamma 2^{s-1}} c^{\gamma 2^{s-2}} \equiv +1 \pmod{p}.$$

For $s \geq 3$, set $\epsilon_1=0$ or 1 according as the square root of the left member is $\equiv +1$ or -1 . Then

$$g^{\epsilon_1 \gamma 2^{s-1} + \epsilon_0 \gamma 2^{s-2}} c^{\gamma 2^{s-3}} \equiv +1 \pmod{p}.$$

Proceeding similarly, we ultimately get

$$g^{2^e \gamma} c^\gamma \equiv +1 \pmod{p}, \quad e = \epsilon_0 + 2\epsilon_1 + \dots + 2^{s-2}\epsilon_{s-2}.$$

Thus $x \equiv \pm g^e c^{(\gamma+1)/2} \pmod{p}$. Then $X^2 \equiv c \pmod{p^\lambda}$ has the root

$$X \equiv x p^{\lambda-1} c^{(p^\lambda - 2p^{\lambda-1} + 1)/2} \pmod{p^\lambda}.$$

G. B. Mathews⁷⁷ (p. 53) treated the cases in which $x^2 \equiv a \pmod{p}$ is solvable by formulas. Cf. Legendre.¹⁵⁶

S. Dickstein¹⁹⁴ noted that H. Wronski¹⁶⁹ gave the solution

$$y = hK + (-1)^{k+1} + Mi, \quad z = h + (-1)^{\pi+k} A \left[\frac{M}{K}, \pi \right]^{(\pi-1)} + Mj$$

of $z^n - ay^n \equiv 0 \pmod{M}$ with $(1^{k/1})^2$ in place of K , and gave, as the condition for solvability,

$$a(1^{k/1})^{2n} - 1 \equiv 0 \pmod{M}.$$

But there may be solutions when the last condition is satisfied by no integer k . This is due to the fact that the value assigned to y imposes a limitation, which may be avoided by using the same expressions for y, z in a parameter K , subject to the condition $aK^n - 1 \equiv 0 \pmod{M}$.

M. F. J. Mann^{194a} proved that, if $n = 2^k \lambda^a \mu^b \dots$, where λ, μ, \dots are distinct odd primes, the number of solutions of $x^n \equiv 1 \pmod{n}$ is $GG_1G_2 \dots g_1g_2 \dots$, where $G = 1$ if n or p is odd, otherwise G is the g. c. d. of $2p$ and 2^{k-1} , and where $G_1, G_2, \dots, g_1, g_2, \dots$ are the g. c. d.'s of p with $\lambda^{a-1}, \mu^{b-1}, \dots, \lambda-1, \mu-1, \dots$, respectively.

A. Tonelli¹⁹⁵ gave an explicit formula for the roots of $x^2 \equiv c \pmod{p^\lambda}$,

¹⁹¹Casopis, Prag, 18, 1889, 97; cf. Fortschritte Math., 1889, 30.

¹⁹²Denkschriften Ak. Wiss. Wien (Math.), 57, 1890, 520.

¹⁹³Göttingen Nachrichten, 1891, 344-6.

¹⁹⁴Bull. Internat. de l'Acad. Sc. de Cracovie, 1892, 372 (64-65); Berichte Krakauer Ak. Wiss., 26, 1893, 155-9.

^{194a}Math. Quest. Educ. Times, 56, 1892, 24-7.

¹⁹⁵Atti R. Accad. Lincei, Rendiconti, (5), 1, 1892, 116-120.

when p is an odd prime, and a quadratic non-residue g of p is known. Set $p = 2^s a + 1$, where $s \geq 1$ and a is odd. Then $\gamma = ap^{\lambda-1}$ is odd, and $\phi(p^\lambda) = 2^s \gamma$. Tonelli's earlier work for modulus p now holds for modulus p^λ and we get $x \equiv \pm g^{e\gamma} c^{(\gamma+1)/2}$. If $s = 1$, then $e = 0$ and the root is that given by Lagrange if $\lambda = 1$. If $s = 2$, whence $p = 4a + 1 = 8l + 5$, the expression for x is given a form free of $e = e_0$:

$$x \equiv \pm (c^a + 3)^{\gamma} c^{(\gamma+1)/2}, \quad \gamma = ap^{\lambda-1}.$$

A. Tonelli¹⁹⁶ expressed the root x in a form free of e for every s :

$$x \equiv \pm v_0^{\gamma 2^{s-2}} v_1^{\gamma 2^{s-3}} \dots v_{s-3}^{2\gamma} v_{s-2}^{\gamma} c^{\frac{\gamma+1}{2}},$$

where the v 's are given by the recursion formula

$$v_{s-h} = c^{2^{s-h} a} v_{s-2}^{2^{s-h+1} a} \dots v_{s-h+1}^{2^{s-2} a} + k \quad (h = 2, 3, \dots).$$

Here k is an existing integer such that $k+1$ is a quadratic residue of p , and $k-1$ a non-residue. Thus, if $s = 3$,

$$x \equiv \pm (c^{2a} + k)^{\gamma} \{ (c^{2a} + k)^{2a} c^a + k \}^{\frac{\gamma+1}{2}},$$

where we may take $k = -2$ if a is not divisible by 3, but $k = -4$ if a is divisible by 3, while neither a nor $4a+1$ are divisible by 5.

N. Amici⁸⁶ proved that $x^{2^k} \equiv b \pmod{2^r}$, b odd, $k \leq r-2$, is solvable only when b is of the form $2^{k+2}h+1$ and then has 2^{k+1} roots, as shown by use of indices. For $(x^m)^{2^k} \equiv b$, the same condition on b is necessary; thus it remains to solve $x^m \equiv \beta \pmod{2^r}$ when m is odd. If $\beta = 8k+1$ or $8k+3$, it has an index to the base $8h+3$ and we get an unique root. If $\beta = 8k-3$ or $8k-1$, then $x^m \equiv -\beta$ has a root a by the preceding case, and $-a$ is a root of the proposed congruence.

Jos. Mayer¹⁹⁷ found the number of roots of $x^3 \equiv a \pmod{p^n}$, for the primes 2, 3, $p = 6m \pm 1$. If a_1, a_2, \dots are residues of n th powers modulo p , and if q is the g. c. d. of n and $p-1$, then $a_1 a_2 \dots \equiv +1$ or $-1 \pmod{p}$, according as $p' = (p-1)/q$ is odd or even. If p' is even, we can pair the numbers belonging to the exponent p' so that the sum of a pair is 0 or p ; hence there exists a residue of an n th power $\equiv -1 \pmod{p}$; but none if p' is odd.

K. Zsigmondy⁸⁷ obtained by the use of abelian groups known theorems on the number, product and sum of the roots of $x^d \equiv 1 \pmod{m}$.

G. Speckmann¹⁹⁸ considered $x^2 \equiv a \pmod{p}$, where p is an odd prime. Set $P = (p-1)/2$. When they exist, the roots may be designated $P-k, P+1+k$, whose sum is p . The successive differences of $P^2, (P+1)^2, (P+2)^2, \dots$ are $p, p+2, p+4, \dots$. The sum of $z = s+1$ terms of 2, 4, 6, \dots is $s^2 + 3s + 2 = z^2 + z$. Adding to the latter the remainder r obtained by dividing P^2 by p , we must get $pn + a$. Hence in $pn + a - r$ we give to n the values

¹⁹⁶Atti R. Accad. Lincei, Rendiconti, (5), 2, 1893, 259-265.

¹⁹⁷Ueber nte Potenzreste und binomische Congruenzen dritten Grades, Progr., Freising, 1895.

¹⁹⁸Archiv Math. Phys., (2), 14, 1896, 445-8; 15, 1897, 335-6.

0, 1, 2, . . . until we reach a number of the form z^2+z (found by extracting the square root). Then $k=z$, so that the roots $P-k$, $P+1+k$ are found.

N. Amici¹⁹⁹ proved that if neither m nor b is divisible by the prime p , and if a is a given root of $x^m \equiv b \pmod{p}$, and if β , q are (existing) integers such that

$$\beta\phi(p^\lambda) - p^{\lambda-1} + 1 = mq,$$

then $a^{p^{\lambda-1}b^q}$ is a root of $x^m \equiv b \pmod{p^\lambda}$. Hence we limit attention to the case $\lambda=1$. Consider henceforth $x^{2^k} \equiv b \pmod{p}$, where $p=2^sh+1$ is an odd prime, h being odd, and b not divisible by p . First, let $k \geq s$. Then $b^h \equiv 1 \pmod{p}$ is a necessary and sufficient condition for solvability and $x \equiv \pm b^q$ are roots, where q is such that $2^k q - 1$ is divisible by h . If g is a quadratic non-residue of p , all 2^s roots are given by $\pm b^q g^{he}$, where $e = \epsilon_1 + 2\epsilon_2 + \dots + 2^{s-2}\epsilon_{s-1}$, the ϵ_i taking the values 0 and 1 independently. Finally, let $k < s$. Then two roots $\pm\beta$ are determined by the method of Tonelli, while all the roots are given by

$$x \equiv \pm \beta g^{ht}, \quad t = \epsilon_1 + 2\epsilon_2 + \dots + 2^{k-2}\epsilon_{k-1}, \quad \epsilon_i = 0 \text{ or } 1.$$

R. Alagna²⁰⁰ considered a prime $p=4k+1$ for which k is a prime. Since 2 is known to be a primitive root of p , it is easy to write down those powers of 2 which give all the roots of $x^d \equiv 1 \pmod{p}$, where d is one of the six divisors 2^i or $2^i k$ of $p-1$, likewise of $x^d \equiv N$, since N must be congruent to an even power of 2. For the modulus p^λ , we may apply the first theorem of Amici or proceed directly. The same questions are treated for a prime $4k+3$ for which $2k+1$ is a prime.

A. Cunningham²⁰¹ treated at length the solution of $x^l \equiv 1 \pmod{N^t}$, where N is a prime, and gave tables showing all incongruent roots when $t=1, 2$, $N \leq 101$, l any admissible divisor of $N-1$; also for a few additional t 's when N is small.

Cunningham^{201a} treated $a^p \equiv 1 \pmod{q^2}$ and $3 \cdot 2^x \equiv \pm 1 \pmod{p}$. He^{201b} treated the problem to find $b^y \equiv +1$ or $\pm a$, given $a^\xi \equiv 1$, $a^x \equiv \pm b \pmod{p}$, where ξ is odd and ξ, x, y are the least values of their kind; also given $a^\xi \equiv 1$, $a^x \equiv \pm b$, $a^y \equiv \pm c$, to find the least β and γ such that $b^\beta \equiv c$, $c^\gamma \equiv b \pmod{p}$.

W. H. Besant²⁰² would solve $y^2 = ax+b$ by finding the roots s of $s^2 \equiv b \pmod{a}$. Then $y = ar+s$, $x = ar^2 + 2rs + (s^2-b)/a$.

G. Speckmann²⁰³ replaced $x^n \equiv k \pmod{p}$ by the pair of congruences $x^{n-1} \equiv r$, $rx \equiv k \pmod{p}$. In $np+k$ give to n the values 0, 1, 2, . . . until we find one for which $np+k=rx$ such that, by trial, $x^{n-1} \equiv r$. The method is, of course, impractical.

¹⁹⁹Rendiconti Circolo Mat. di Palermo, 11, 1897, 43-57.

²⁰⁰Rendiconti Circolo Mat. di Palermo, 13, 1899, 99-129.

²⁰¹Messenger of Math., 29, 1899-1900, 145-179. Errata, Cunningham²²⁶, p. 155. See 13a of Ch. IV.

^{201a}Math. Quest. Educ. Times, 71, 1899, 43-4; 75, 1901, 52-4.

^{201b}Ibid., (2), 1, 1902, 70-2.

²⁰²Math. Gazette, 1, 1900, 130.

²⁰³Archiv Math. Phys., (2), 17, 1900, 110-2, 120-1.

G. Picou²⁰⁴ applied to the case $n=2$ Wronski's¹⁶⁹ formula for the residues of n th powers modulo M , M arbitrary. For example, if $M=16a\pm 1$,

$$(h\pm 8a)^2\equiv \mp a(4h-1)^2 \pmod{M}.$$

[If $8a$ were replaced by $4a$, we would have an identity in h .]

P. Bachmann¹⁰⁴ (pp. 344-351) discussed $x^m\equiv a \pmod{p^a}$, $p>2$, $p=2$.

G. Arnoux²⁰⁵ solved $x^{14}\equiv 79 \pmod{3\cdot 5\cdot 7}$ by getting the residue 2 of 79 modulo 7 and that of 14 modulo $\phi(7)=6$ and solving $x^2\equiv 2 \pmod{7}$ by use of a table of residues of powers modulo 7. Similarly for moduli 3, 5. Take the product of the roots as usual.

M. Cipolla²⁰⁶ generalized the results of Alagna²⁰⁰ to the case of a prime $p=2^mq+1$, $m>0$, q an odd prime, including unity. For any divisor d of $p-1$, the roots of $x^d\equiv N \pmod{p}$ are expressed as given powers of a primitive root a of p . If 2 belongs to the exponent $2^e\omega$ modulo p , where ω is odd, then $q^e\equiv 1 \pmod{p}$ if and only if 2^{e-1} is the highest power of 2 dividing m .

Cunningham^{206a} found the sum of the roots of $(y^n\pm 1)/(y\pm 1)\equiv 0 \pmod{p}$.

M. Cipolla²⁰⁷ proved the existence of an integer k such that k^2-q is a quadratic non-residue of the prime p not dividing the given integer q . Let

$$u_n = \frac{1}{2}\sqrt{q} \{ (k+\sqrt{q})^n - (k-\sqrt{q})^n \},$$

$$v_n = \frac{1}{2} \{ (k+\sqrt{k^2-q})^n + (k-\sqrt{k^2-q})^n \}.$$

By expansion of the binomials it is shown that the roots of $x^2\equiv q \pmod{p}$ are given by $\pm u_{(p-1)/2}$ and by $\pm v_{(p+1)/2}$. These may be computed by use of

$$w_n \equiv 2kw_{n-1} - qw_{n-2} \pmod{p} \quad (w=u \text{ or } v),$$

with the initial values $u_0=1$, $u_1=p$; $v_0=1$, $v_1=k$. Although u_n , v_n are the functions of Lucas, the exposition is here simple and independent of the theory of Lucas (Ch. XVII).

M. Cipolla²⁰⁸ proved that if q is a quadratic residue and k^2-q is a quadratic non-residue of an odd prime p , $z^2\equiv q \pmod{p^\lambda}$ has the roots

$$\pm \frac{1}{2}\sqrt{q} \{ (k+\sqrt{q})^r - (k-\sqrt{q})^r \},$$

where $r=p^{\lambda-1}(p-1)/2$. Other expressions for the roots are

$$\pm \frac{1}{2}q' \{ (k+\sqrt{k^2-q})^s + (k-\sqrt{k^2-q})^s \},$$

$$t=(p^\lambda-2p^{\lambda-1}+1)/2, \quad s=p^{\lambda-1}(p+1)/2.$$

Thus if $z_1^2\equiv q \pmod{p}$, the roots modulo p^λ are $\pm q'z_1^{p^{\lambda-1}}$ (Tonelli¹⁹³). Finally, let $n=\prod p_i^{\lambda_i}$, where the p 's are primes >3 ; take $\epsilon_i=\pm 1$ when $p_i\equiv \mp 1 \pmod{4}$. There exists a number Δ of the form k^2-q such that

²⁰⁴L'intermédiaire des math., 8, 1901, 162.

²⁰⁵Assoc. franç. av. sc., 31, 1902, II, 185-201.

²⁰⁶Periodico di Mat., 18, 1903, 330-5.

^{206a}Math. Quest. Educ. Times, (2), 4, 1903, 115-6; 5, 1904, 80-1.

²⁰⁷Rendiconto Accad. Sc. Fis. e Mat. Napoli, (3), 9, 1903, 154-163.

²⁰⁸Ibid., (3), 10, 1904, 144-150.

$(\Delta/p_1) = \epsilon_1, \dots, (\Delta/p_\nu) = \epsilon_\nu$, where the symbols are Legendre's. Call M the l. c. m. of $p_i^{N-1}(p_i - \epsilon_i)/2$ for $i=1, \dots, \nu$. Then $z^2 \equiv q \pmod{n}$ has the root

$$\frac{1}{2}q^{\frac{1}{2}(\varphi(n)-M+1)/2} \{ (k + \sqrt{\Delta})^M + (k - \sqrt{\Delta})^M \}.$$

A. Cunningham²⁰⁹ indicated how his tables may be used to solve directly $x^n \equiv -1 \pmod{p}$ for $n=2, 3, 4, 6, 12$. From $p = a^2 + b^2$, we get the roots $x \equiv \pm a/b$ of $x^2 \equiv -1 \pmod{p}$. Also $p = a^2 + b^2 = c^2 + 2d^2$ gives the roots $\pm d(a+b)/(ce)$ and $\pm c(a \pm b)/(2de)$ of $x^4 \equiv -1 \pmod{p}$, where $e = a$ or b . Again, $p = A^2 + 3B^2$ gives the roots $(A-B)/(2B)$, $(B+A)/(B-A)$, and their reciprocals, of $x^3 \equiv 1 \pmod{p}$.

M. Cipolla¹⁰⁷ gave a report (in Peano's symbolism) on binomial congruences.

M. Cipolla²¹⁰ proved that if p is an odd prime not dividing q and if $z^2 \equiv q \pmod{p}$ is solvable, the roots are

$$z \equiv \pm 2(qs_1 + q^2s_3 + q^3s_5 + \dots + q^{(p-3)/2}s_{p-4} + s_{p-2})$$

where

$$s_r = 1^r + 2^r + \dots + \left(\frac{p-1}{2}\right)^r.$$

Then $x^2 \equiv q \pmod{p^\lambda}$ has the root $z^{p^{\lambda-1}}q^e$, $e = (p^\lambda - 2p^{\lambda-1} + 1)/2$. For $p \equiv 1 \pmod{4}$, $x^4 \equiv q \pmod{p}$ has the root

$$4 \sum_{i=1}^{2l} q^i s_{2i-1} \cdot \sum_{j=1}^l q^{j-1} s_{4j-3} + 2 \sum_{i=1}^l q^i s_{4i-1} \quad \left(l = \frac{p-1}{4}\right).$$

M. Cipolla²¹¹ extended the method of Legendre¹⁵⁹ and proved that

$$x^{2^m} \equiv 1 + 2^s A \pmod{2^k},$$

for A odd and $s \geq m+2$, has a root

$$x = 1 + 2^s A c_1 - 2^{2s} A^2 c_2 + \dots + (-1)^{n-1} 2^{ns} A^n c_n, \quad n = \left\lfloor \frac{k-2}{s-m-1} \right\rfloor,$$

where

$$c_1 = \frac{1}{2^m}, \quad c_n = \frac{(2^m - 1)(2 \cdot 2^m - 1) \dots (n-1 \cdot 2^m - 1)}{2^{mn} n!}$$

are the coefficients in

$$(1+z)^{1/2^m} = 1 + c_1 z - c_2 z^2 + c_3 z^3 - \dots - (-1)^n c_n z^n + \dots$$

O. Meissner²¹² gave for a prime $p = 8n + 5$ the known root

$$\xi = D^{\frac{p+3}{8}} \text{ of } x^2 \equiv D \pmod{p}, \quad D^{\frac{p-1}{4}} \equiv 1 \pmod{p}.$$

But if $D^{(p-1)/4} \equiv -1 \pmod{p}$, a root is $\xi \{ (p-1)/2 \}!$, since the square of the last factor is congruent to $(-1)^{(p+1)/2}$ by Wilson's theorem.

Tamarkine and Friedmann²¹³ expressed the roots of $z^2 \equiv q \pmod{p}$ by a formula, equivalent to Cipolla's,²¹⁰

²⁰⁹Quadratic Partitions, 1904, Introd., xvi-xvii. Math. Quest. Educ. Times, 6, 1904, 84-5; 7, 1905, 38-9; 8, 1905, 18-9.

²¹⁰Rendiconto Accad. Sc. Fis. e Mat. Napoli, (3), 11, 1905, 13-19.

²¹¹Ibid., 304-9.

²¹²Archiv Math. Phys. (3), 9, 1905, 96.

²¹³Math. Annalen, 62, 1906, 409.

$$z \equiv \pm 2 \sum_{m=0}^{(p-3)/2} q^{1/2(p-1)-m} s_{2m+1}.$$

For, according as y^2 is or is not $\equiv q \pmod{p}$, we have

$$y \{1 - (y^2 - q)^{p-1}\} \equiv y \text{ or } 0 \pmod{p}.$$

We can express s_{2m+1} in terms of Bernoullian numbers.

A. Cunningham²¹⁴ gave a tentative method of solving $x^2 \equiv a \pmod{p}$. He^{214a} noted that a root $Y = 2\eta^2$ of $Y^4 \equiv -1$ leads to the roots of $y^8 \equiv -1 \pmod{p}$.

M. Cipolla²¹⁵ employed an odd prime p and a divisor n of $p-1 = nv$. If r_1, \dots, r_v form a set of residues of p whose n th powers are incongruent, and if $q^r \equiv 1 \pmod{p}$, then $x^n \equiv q \pmod{p}$ has the root

$$x \equiv \sum_{k=0}^{v-1} A_k q^k, \quad A_k = -n \sum_{j=1}^v r_j^{nk-1}.$$

For $n=2$, this becomes his²¹⁰ earlier formula by taking $1, 2, \dots, (p-1)/2$ as the r 's. Next, let $p-1 = m\mu$, where m and μ are relatively prime and m is a multiple of n . If γ and δ belong to the exponents m and μ modulo p , the products $\gamma^r \delta^s$ ($r < m/n$, $s < \mu$) may be taken as r_1, \dots, r_v . According as $nk \equiv 1$ or not $\pmod{\mu}$, we have

$$A_k \equiv -n\mu \frac{\gamma^{(nk-1)m/n} - 1}{\gamma^{nk-1} - 1} \text{ or } A_k \equiv 0 \pmod{p}.$$

If n is a prime and n^r is its highest power dividing $p-1$, there exists a number ω not an n th power modulo p and we may set $m = n^r$, $\gamma \equiv \omega^\mu \pmod{p}$. In particular, if $n=2$, $x^2 \equiv q$ has the root

$$x \equiv \frac{-1}{2^{r-2}} q^{\frac{p+2^r-1}{2^{r+1}}} \sum_{s=0}^{2^r-1-1} q^{s(p-1)/2^r} / (\omega^{(2s+1)(p-1)/2^r} - 1),$$

where ω is a quadratic non-residue of p . If $p \equiv 5 \pmod{8}$, we may take $\omega = 2$ and get

$$\frac{1}{2} q^{\frac{p+3}{8}} \{2^t + 1 - (2^t - 1)q^t\}, \quad t = \frac{p-1}{4}.$$

M. Cipolla²¹⁶ considered the congruence, with p an odd prime,

$$x^{p^r} \equiv a \pmod{p^m}, \quad r < m,$$

a necessary condition for which is that $h = (a^{p^r} - a)/p^{r+1}$ be an integer. Determine A by $a^{p^r} A \equiv h \pmod{p^m}$. Then the given congruence has the root ax_0 if x_0 is a root of

$$x^{p^r} \equiv 1 - Ap^{r+1} \pmod{p^m}.$$

This is proved to have the root

²¹⁴Math. Quest. Educ. Times, (2), 13, 1908, 19-20.

^{214a}*Ibid.*, 10, 1906, 52-3.

²¹⁵Math. Annalen, 63, 1907, 54-61.

²¹⁶Atti R. Accad. Lincei, Rendiconti, (5), 16, I, 1907, 603-8.

$$x_0 = 1 - \sum_{i=1}^k c_i A^i p^{i(r+1)}, \quad k = m+1 + \left[\frac{m-2}{p-2} \right],$$

where $c_1 = 1/p^r, \dots$ are given by the expansion

$$\sqrt[p^r]{1-z} = 1 - c_1 z - c_2 z^2 - \dots$$

M. Cipolla²¹⁷ treated $x^n \equiv a \pmod{p^m}$ where n divides $\phi(p^m)$. We may set $n = p^r \nu$, where ν divides $p-1$. Determine integers α, β such that

$$\alpha p^r + \nu \beta \equiv 1 \pmod{p^{m-r-1}(p-1)}.$$

Then the initial congruence has the root yx_1^α if $y^{p^r} \equiv a^\beta \pmod{p^m}$, solved as in his preceding paper, and if x_1 is a root of $x^\nu \equiv a \pmod{p^m}$. The latter has the root

$$\frac{1}{t} a^{(p^m - 2p^{m-1} + 1)/\nu} \sum_{k=0}^{t-1} a^{kp^{m-1}} \sum_{i=1}^t \rho_i^{\nu k-1},$$

where $t = (p-1)/\nu$, $\rho_i \equiv r_i^{p^{m-1}} \pmod{p^m}$, r_1, \dots, r_t being integers prime to p such that their ν th powers are incongruent and form a group modulo p^m .

K. A. Posse²¹⁸ gave a simplified exposition of Korkine's¹¹⁸ method of solving binomial congruences. Cf. Posse,¹²⁹ Schuh.¹²³⁻⁴

F. Stasi²¹⁹ proved that we obtain all solutions of $x^2 \equiv a^2 \pmod{n}$, where n is odd and prime to a , by expressing n as a product of two relatively prime factors P and Q in all ways, setting $x - a = Pz$ and finding z from $Pz + 2a \equiv 0 \pmod{Q}$. [Instead of his very long proof, it may be shown at once that we may take $x - a, x + a$ divisible by P, Q , respectively.]

L. Grossschmid²²⁰ gave for the incongruent roots of $x^2 \equiv r \pmod{M}$ an explicit formula obtained by means of the ideal factors of M in a quadratic number-field.

L. Grossschmid²²¹ treated the roots of quadratic binomial congruences.

A. Cunningham²²² solved $x^2 \equiv -1 \pmod{p}$, where $p = 616318177$ is a prime factor of $2^{37} - 1$; by using various small moduli, he obtained $p = 24561^2 + 3616^2$.

L. von Schrutka^{222a} used a correspondence between the integers and certain rational numbers to treat quadratic congruences without novelty as to results. The method will be given under the topic Fields in a later volume of this History.

Grossschmid²²³ employed the products R and N of all the quadratic residues and non-residues, respectively, $\leq 2n$ of a prime $p = 4n + 1$. Then

$$R^2 \equiv (-1)^{n+1}, \quad N^2 \equiv (-1)^n \pmod{p}.$$

²¹⁷Atti R. Accad. Lincei, Rendiconti, (5), 16, I, 1907, 732-741.

²¹⁸Charikov Soobšč. Mat. Obšč. (Report Math. Soc. Charkov), (2), 11, 1910, 249-268 (Russian).

²¹⁹Il Boll. Matematica Gior. Sc.-Didat., 9, 1910, 296-300.

²²⁰Jour. für Math., 139, 1911, 101-5.

²²¹Math. és Phys. Lapok, Budapest, 20, 1911, 47-72 (Hungarian).

²²²Math. Questions Educat. Times, (2), 20, 1911, 33-4 (76).

^{222a}Monatshefte Math. Phys., 23, 1912, 92-105.

²²³Archiv Math. Phys., (3), 21, 1913, 363; 23, 1914-5, 187-8.

Hence $\pm R$ and $\pm N$ are the roots of $x^2 \equiv -1 \pmod{p}$ according as $p = 8m+1$ or $8m+5$.

U. Concina²²⁴ proved the first result by Legendre.¹⁵⁴

A. Cunningham²²⁵ tabulated the roots of $y^4 \equiv \pm 2$, $2y^4 \equiv \pm 1 \pmod{p}$, for each prime $p < 1000$.

Cunningham²²⁶ listed the roots of $y^l \equiv \pm 1 \pmod{p^*}$, where $l = qp^a$, p being an odd prime ≤ 19 , $p^* < 10^4$, $a = 1$ and often also $a = 2$, q a factor of $p-1$.

A. Gérardin and L. Valroff²²⁷ solved $2y^4 \equiv 1 \pmod{p}$, $1000 < p < 5300$.

Cunningham²²⁸ announced the completion of tables giving all proper roots of $y^m \equiv 1 \pmod{p^k}$ for m odd ≤ 15 , and of $y^m \equiv -1 \pmod{p^k}$ for m even ≤ 14 . These tables have since been completed up to $p^k < 100000$ and are now nearly all in type.

T. G. Creak²²⁸ announced the completion of like tables for $m = 16$ to 50 ; 52 , 54 , 56 , 63 , 64 , 72 , 75 , and $10^3 < p^k < 10^4$.

H. C. Pocklington²²⁹ noted that if p is a prime $8m+5$ and $a^{2m+1} \equiv -1$, $x^2 \equiv a \pmod{p}$ has the roots $\pm \frac{1}{2}(4a)^{m+1}$. He showed how to use $(t + u\sqrt{D})^n$ to solve $x^2 \equiv -D \pmod{p = 4k+1}$, and treated $x^3 \equiv a$.

*J. Maximoff²³⁰ treated binomial congruences and primitive roots.

*G. Rados²³¹ gave a new proof of known criteria for the solvability of $x^2 \equiv D \pmod{p}$. He²³² gave a new exposition of the theory of binomial congruences without using indices.

Congruences $x^{p-1} \equiv 1 \pmod{p^n}$ are treated in Chapter IV. Euler^{4, 7} of Ch. XVI solved $x^2 \equiv -1 \pmod{p}$. Lazzarini¹⁷² of Ch. I erred on the number of roots of $z^2 \equiv -3 \pmod{n}$. Many papers in Ch. XX treat $x^k \equiv x \pmod{10^n}$. The following papers from the first part of Ch. VII treat also binomial congruences: Euler,² Lagrange,³ Poinso^t,¹¹ Cauchy,¹⁴ Lebesgue,⁵⁹ Epstein,¹¹² Korkine.¹¹⁸

²²⁴Periodico di Mat., 28, 1913, 212-6.

²²⁵Messenger Math., 43, 1913-4, 52-3.

²²⁶*Ibid.*, 148-163. Cf. Cunningham.²⁰¹

²²⁷Sphinx-Oedipe, 1913, 34; 1914, 18-37, 73.

²²⁸Messenger Math., 45, 1915-6, 69.

²²⁹Proc. Cambridge Phil. Soc., 19, 1917, 57-9.

²³⁰Bull. Soc. Phys.-Math. Kasan, (2), XXI.

²³¹Math. és Termés. Értésítő, 33, 1915, 758-62.

²³²*Ibid.*, 34, 1916, 641-55.

CHAPTER VIII.

HIGHER CONGRUENCES.

A CONGRUENCE OF DEGREE n HAS AT MOST n ROOTS IF THE
MODULUS p IS A PRIME.

J. L. Lagrange¹ proved that, if a is not divisible by the prime p , $ax^n + bx^{n-1} + \dots$ is divisible by p for at most n integers x between $p/2$ and $-p/2$. For, let $a, \beta, \dots, \rho, \sigma$ be $n+1$ such distinct integers. Then the quotient of

$$a(x^n - a^n) + b(x^{n-1} - a^{n-1}) + \dots$$

by $x - a$ is a polynomial $ax^{n-1} + \dots$ which is divisible by p when $x = \beta, \dots, \sigma$. Proceeding as before, we finally have $a(\rho - \sigma)$ divisible by p , which is impossible.

L. Euler² noted that $x^n - 1$ is divisible by a prime p for not more than n integers x , $0 < x < p$. For, if $x = a$, is such an integer, then $x - a$ divides $x^n - 1 - mp$, where m is a suitable integer; the quotient f is of degree $n - 1$. If $x = b$ is a second such integer, $x - b$ divides $f - m'p$. Proceeding as in algebra, we obtain the theorem stated. [The argument is applicable to any polynomial of degree n in x .]

A. M. Legendre³ noted that $P \equiv (x - a)Q + pA$ has only one more root than Q .

C. F. Gauss⁴ proved the theorem by assuming that there is a congruence $ax^n + \dots \equiv 0 \pmod{p}$ with more than n roots a, \dots , and that every congruence of degree l , $l < n$, has at most l roots. Substituting $y + a$ for x , we obtain a congruence $ay^n + \dots \equiv 0$ with more than n roots, one of which is zero. Removing the factor y , we obtain $ay^{n-1} + \dots \equiv 0$ with more than $n - 1$ roots, contrary to hypothesis.

Gauss⁵ noted that if a is a root of $\xi \equiv 0 \pmod{p}$, then ξ is divisible by $x - a$ modulo p . If a, b, \dots are incongruent roots, ξ is divisible modulo p by the product $(x - a)(x - b) \dots$. Hence the number of roots does not exceed the degree of ξ .

A. Cauchy⁶ made the proof by use of $X \equiv (x - a)X_1 \pmod{p}$, identically in x , where the degree of X_1 is one less than the degree of X .

A. L. Crelle⁷ and S. Earnshaw⁸ gave Lagrange's proof.

Crelle⁹ proved that if e_1, \dots, e_n are n distinct roots,‘

$$ax^n + \dots \equiv a(x - e_1) \dots (x - e_n) + pN.$$

¹Mém. Ac. Berlin, 24, année 1768 (1770), p. 192; Oeuvres, 2, 1868, 667-9.

²Novi Comm. Ac. Petrop., 18, 1773, p. 93; Comm. Arith., 1, 519-20.

³Mém. Ac. Roy. Sc., Paris, 1785, 466; Théorie des nombres, 1798, 184.

⁴Disq. Arith., 1801, Art. 43.

⁵Posthumous paper, Werke, 2, p. 217, Art. 338 (p. 214, Art. 333). Maser's German translation of Gauss' Disq. Arith., etc., 1889, p. 607 (p. 604).

⁶Exercices de Math., 4, 1829, 219; Oeuvres, (2), 9, 261; Comptes Rendus Paris, 12, 1841, 831-2; Exercices d'Analyse et de Phys. Math., 2, 1841, 1-40, Oeuvres, (2), 12.

⁷Berlin Abhand., Math., 1832, p. 34.

⁸Cambridge Math. Jour., 2, 1841, 79.

⁹Berlin Abhand., Math., 1843, 50-54.

L. Poinso¹⁰ gave the proof due to Crelle.⁹

J. A. Grunert¹¹ proceeded by induction from $n-1$ to n , making use of the first part of Lagrange's proof.

D. A. da Silva¹² gave a proof.

NUMBER OF ROOTS OF HIGHER CONGRUENCES.

G. Libri¹⁶ found that $f(x, y, \dots) \equiv 0 \pmod{m}$ has

$$\frac{1}{m} \sum_{x=a}^b \sum_{y=c}^d \dots \left\{ \sum_{k=0}^{m-1} \cos \frac{2k\pi f}{m} + i \sin \frac{2k\pi f}{m} \right\}$$

sets of solutions such that $a \leq x \leq b$, $c \leq y \leq d, \dots$. The total number of sets of solutions is

$$\frac{1}{m} \sum_{x=0}^m \sum_{y=0}^m \dots \left\{ 1 + \cos \frac{2\pi f}{m} + \cos \frac{4\pi f}{m} + \dots + \cos 2 \frac{(m-1)\pi f}{m} \right\}.$$

V. A. Lebesgue¹⁷ proved that if p is a prime we obtain as follows the residue modulo p of the number S_k of sets of solutions of $F(x_1, \dots, x_n) \equiv 0 \pmod{p}$, in which each x_i is chosen from $0, 1, \dots, p-1$, and F is a polynomial with integral coefficients. Let ΣA be the sum of the coefficients of the terms $Ax_1^a \dots x_k^g$ of the expansion of F^{p-1} in which each of the exponents a, \dots, g is a multiple >0 of $p-1$. Then $S_k \equiv (-1)^{k+1} \Sigma A \pmod{p}$.

Henceforth, let $p = hm + 1$. First, let $F = x^m - a$. In F^{p-1} the coefficient of $x^{m(p-1-n)}$ is $\binom{p-1}{n} (-a)^n \equiv a^n \pmod{p}$. The exponent of x will be a multiple >0 of $p-1$ only when $n = k(p-1)/d$, for $k = 0, 1, \dots, d-1$, where d is the g. c. d. of m and $p-1$. Thus $S_1 \equiv \Sigma a^{k(p-1)/d} \pmod{p}$, while evidently $S_1 < p$. According as $a^{(p-1)/d} \equiv 1$ or not, we get $S_1 = d$ or 0 .

Next, let $F = x^m - ay^m - b$. Set $c = ay^m + b$. In $(x^m - c)^{p-1}$ we omit the terms in which the exponent of x is not a multiple >0 of $p-1$ and also the $x^{m(p-1)}$ not containing y . Since the arithmetical coefficient is $\equiv 1$ as in the first case, we get

$$c^h x^{m(p-1-h)} + c^{2h} x^{m(p-1-2h)} + \dots + c^{(m-1)h} x^{mk}.$$

In this, we replace c^{kh} by those terms of $(ay^m + b)^{kh}$ in which the exponents are multiples >0 of $p-1$, viz.,

$$\sum_{l=0}^{k-1} \binom{kh}{lh} (ay^m)^{kh-lh} b^{lh}.$$

Set $y = 1$, and sum for $k = 1, \dots, m-1$; we get $-S_2 \pmod{p}$. It is shown otherwise that S_2 is a multiple $< mp$ of m .

To these two cases is reduced the solution of

$$(1) \quad F = a_1 x_1^m + \dots + a_k x_k^m \equiv a \pmod{p = hm + 1}.$$

¹⁰Jour. de Mathématiques, 10, 1845, 12-15.

¹¹Klûgel's Math. Wörterbuch, 5, 1831, 1069-71.

¹²Proprietades... Congruencias binomias, Lisbon, 1854. Cf. C. Alasia, Rivista di fisica, mat. e sc. nat., 4, 1903, p. 9.

¹⁶Mém. divers Savants Ac. Sc. de l'Institut de France (Math.), 5, 1838, 32 (read 1825). Jour. für Math., 9, 1832, 54. To be considered in vol. II.

¹⁷Jour. de Math., 2, 1837, 253-292. Cf. vol. 3, 113; vol. 4, 366.

Denote by P the sum of the first f terms of F and by Q the sum of the last $k-f$ terms. Let g be a primitive root of p . Let P^0 be the number of sets of solutions of $P \equiv 0 \pmod{p}$; $P^{(i)}$ the number for $P \equiv g^i \pmod{p}$; Q^0 and $Q^{(i)}$ the corresponding numbers for $Q \equiv 0, Q \equiv g^i$. Then the number of sets of solution of $P \equiv Q \pmod{p}$ is $P^0 Q^0 + h \sum_{i=1}^{p-1} P^{(i)} Q^{(i)}$. Hence we may deduce the number of sets of solutions of $F \equiv 0$ from the numbers for $P \equiv A$ and $Q \equiv -A$. For $F \equiv a$, we employ $P = F$, $Q = g^k x^m$ and get $F^0 = P^0 + (p-1)P^{(k)}$, which determines the desired $P^{(k)}$.

The theory is applied in detail to (1) for $m=2$, k arbitrary, and for $m=3$, 4 , $k=2$. Finally, the method of Libri¹⁶ is amplified.

Th. Schönemann¹⁸ noted that, if S_k is the sum of the k th powers of the roots of an equation $x^n + \dots = 0$ with integral coefficients, that of x^n being unity, and if $S_{(p-1)t} \equiv n \pmod{p}$ for $t=1, 2, \dots, n$, where p is a prime $> n$, the corresponding congruence $x^n + \dots \equiv 0 \pmod{p}$ has n real roots.

A. L. Cauchy¹⁹ considered $F(x) \equiv 0 \pmod{M}$, with $M = AB \dots$, where A, B, \dots are powers of distinct primes. If $F(x) \equiv 0 \pmod{A}$ has α roots, $F(x) \equiv 0 \pmod{B}$ has β roots, etc., the proposed congruence has $\alpha\beta \dots$ roots in all. For, if a, b, \dots are roots for the moduli A, B, \dots and $X \equiv a \pmod{A}$, $X \equiv b \pmod{B}, \dots$, then X is a root for modulus M .

P. L. Tchebychef²⁰ proved that, if p is a prime, a congruence $f(x) \equiv 0 \pmod{p}$ of degree $m < p$ has m roots if and only if the coefficients of the remainder obtained by dividing $x^p - x$ by $f(x)$ are all divisible by p .

Ch. Hermite²¹ proved the theorem: If μ and μ' are the numbers of sets of solutions of $\phi(x, y) \equiv 0$ for the respective moduli M and M' , which are relatively prime, the number of sets of solutions modulo MM' is $\mu\mu'$. If $\phi \equiv 0$ is solvable for a prime modulus p , it will be solvable modulo p^n if

$$\phi \equiv 0, \quad \frac{\partial \phi}{\partial x} \equiv 0, \quad \frac{\partial \phi}{\partial y} \equiv 0 \pmod{p}$$

have no common sets of solutions. In this case, the number of sets of solutions modulo p^n is $p^{n-1}\pi$ if π is the number for modulus p . Similar results are said to hold for any number k of unknowns. If M is a product of powers of the distinct primes p_1, \dots, p_n , and if π_i is the number of sets of solutions of the congruence modulo p_i , then the number of sets for modulus M is

$$M^{k-1} \frac{\pi_1 \dots \pi_n}{(p_1 \dots p_n)^{k-1}}.$$

For $x^2 + Ay^2 \equiv \Delta \pmod{M}$, we have $\pi_i = p_i - (-A/p_i)$, where (a/p) is ± 1 according as a is a quadratic residue or non-residue of p .

Julius König gave a theorem in a seminar at the Technische Hochschule in Budapest during the winter, 1881-2, which was published in the following paper and that by Rados.²⁴

¹⁸Jour. für Math., 19, 1839, 293.

¹⁹Comptes Rendus Paris, 25, 1847, 36; Oeuvres, (1), 10, 324.

²⁰Theorie der Congruenzen, in Russian, 1849; in German, 1889, §21.

²¹Jour. für Math., 47, 1854, 351-7; Oeuvres, 1, 243-250.

G. Raussnitz²³ proved the theorem, due to König: Let

$$(2) \quad f(x) = a_0 x^{p-2} + a_1 x^{p-3} + \dots + a_{p-2},$$

where the a 's are integers and a_{p-2} is not divisible by the prime p . Then $f(x) \equiv 0 \pmod{p}$ has real roots if and only if the cyclic determinant

$$(3) \quad D = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_{p-3} & a_{p-2} \\ a_1 & a_2 & a_3 & \dots & a_{p-2} & a_0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{p-2} a_0 & a_1 & \dots & a_{p-4} & a_{p-3} \end{vmatrix}$$

is divisible by p . In order that it have at least k distinct real roots it is necessary that all $p-k$ rowed minors of D be divisible by p . If also not all $p-k-1$ rowed minors are divisible by p , the congruence has exactly k distinct real roots.

The theorem is applicable to any congruence not having the root zero, since we may then reduce the degree to $p-2$ by Fermat's theorem.

Gustav Rados²⁴ proved König's theorem, using the fact that a system of $p-1$ linear homogeneous congruences modulo p in $p-1$ unknowns has at least k sets of solutions linearly independent modulo p if and only if the $p-k$ rowed minors are divisible by p .

L. Kronecker²⁵ noted that, if p is a prime, the condition for the existence of exactly $p-m-1$ roots of (2), distinct from one another and from zero, is that the rank of the system

$$(3') \quad (a_{i+k}) \quad (i, k = 0, 1, \dots, p-2)$$

modulo p is exactly m , where $a_{s+p-1} = a_s$. The same is the condition for the existence of a $(p-m-1)$ -fold manifold of sets of solutions of the system of linear congruences

$$\sum_{k=0}^{p-2} a_{h+k} \phi_k \equiv 0 \pmod{p} \quad (h = 0, 1, \dots, p-2).$$

L. Kronecker²⁶ gave a detailed proof of his preceding results, noted that the rank is m if not all principal m -rowed minors are divisible by p while all $m+1$ rowed minors are, and added that $c_0 + c_1 x + \dots + c_{p-2} x^{p-2} \equiv 0 \pmod{p}$ has exactly s roots $\neq 0$ if one and the same linear homogeneous congruence holds between every set of $p-s$ (but not fewer) successive terms of the periodic series $c_0, c_1, \dots, c_{p-2}, c_0, c_1, \dots$.

L. Gegenbauer²⁷ proved Kronecker's version of König's theorem.

Gegenbauer²⁸ noted that Kronecker's theorems imply the corollary:

²³Math. und Naturw. Berichte aus Ungarn, 1, 1882-3, 266-75.

²⁴Jour. für Math., 99, 1886, 258-60; Math. Termes Ertesito, Magyar Tudon Ak., Budapest, 1, 1883, 296; 3, 1885, 178.

²⁵Jour. für Math., 99, 1886, 363, 366.

²⁶Vorlesungen über Zahlentheorie, 1, 1901, 389-415, including several additions by Hensel (pp. 393, 399, 402-3).

²⁷Sitzungsber. Ak. Wiss. Wien (Math.), 95, II, 1887, 165-9, 610-2.

²⁸*Ibid.*, 98, IIa, 1889, p. 32, foot-note. Cf. Gegenbauer.²⁵

There exist exactly $p-m-2$ roots of (2), distinct from one another and from zero, if and only if there exist exactly $p-m-2$ distinct linear homogeneous functions

$$\sum_{h=0}^{p-2} a_{k,h} a_h \quad (k=1, \dots, p-m-2)$$

which remain divisible by p after applying all cyclic permutations of the a_h , so that

$$\sum_{h=0}^{p-2} a_{k,h} a_{i+h} \equiv 0 \pmod{p} \quad \left(\begin{matrix} k=1, \dots, p-m-2 \\ i=0, 1, \dots, p-2 \end{matrix} \right).$$

A simple proof of this corollary is given.

L. Gegenbauer²⁹ noted that the number of roots of $f(x) \equiv 0 \pmod{k}$ is

$$\{f(x), k\} = \sum_{x=0}^{k-1} D(k), \quad D(k) = \left[\frac{|f(x)|}{k} \right] - \left[\frac{|f(x)|-1}{k} \right],$$

since $D(k) = 1$ or 0 according as $f(x)$ is divisible by k or not. Let k_1, \dots, k_δ be a series of increasing positive integers and $g(x)$ any function. In the first equation take $k = k_l$, multiply by $g(k_l)$ and sum for $l = 1, \dots, \delta$. Reversing the order of the summation indices l, x in the new right-hand member, we get

$$\sum_{l=1}^{\delta} \{f(x), k_l\} g(k_l) = \sum_{x=0}^{k_\delta-1} G, \quad G = \sum D(\mu) g(\mu),$$

where in G the summation index μ takes those of the values k_1, \dots, k_δ which exceed x . Thus G represents the sum $G(f(x); k_1, \dots, k_\delta; x)$ of the values of $f(\mu)$ when μ ranges over those of the numbers k_1, \dots, k_δ which exceed x and are divisors of $f(x)$. In particular, if $g(x) = 1$, G becomes the number ψ of the k 's which exceed x and divide $f(x)$.

Let $f(x) = m \pm nx$. Then $f(x) \equiv 0 \pmod{k}$ has (k, n) roots or no root according as m is or is not divisible by the g. c. d. (k, n) of k and n ; let $(k, n; m)$ denote (k, n) or 0 in the respective cases. Then

$$\sum_{l=1}^{\delta} (k_l, n; m) g(k_l) = \sum_{x=0}^{k_\delta-1} G(m \pm nx; k_1, \dots, k_\delta; x).$$

Let $G(a, b)$ denote the sum of the values of $g(\mu)$ when μ ranges over all the divisors $> b$ of a ; $\psi(a, b)$ the number of divisors $> b$ of a . Taking $k_l = l$ for $l = 1, \dots, \delta$, we deduce

$$\sum_{l=1}^{\delta} (l, n; m) g(l) = \sum_{x=0}^{\delta-1} \{G(m \pm nx, x) - G(m \pm nx, \delta)\}.$$

For $g(l) = 1$, this reduces to Lerch's¹⁰⁰ relation (16) in Ch. X. Again,

$$\sum_{x=1}^a \{G(m+nx, x-1) - G(m+nx, b+x)\} = \sum_{\mu=0}^b \{G(m-n\mu, \mu) - G(m-n\mu, \mu+a)\},$$

²⁹Sitzungsberichte Ak. Wiss. Wien (Math.), 98, IIa, 1889, 28-36.

which for $g(x) = 1$ yields the first formula of Lerch. Next, if the k 's are primes and q is a prime distinct from them,

$$\sum_{x=0}^{k_\delta-1} G(x^n - q; k_1, \dots, k_\delta; x) = \sum_{l=1}^{\delta} (k_l - 1, n; q) g(k_l).$$

Finally, he treated $f(x)$ of degree $d = k_\delta - 2$, whose constant term is prime to each k_i and coefficient of x^{d-i} is divisible by the prime k_μ if $i < k_\delta - k_\mu$.

Gegenbauer³⁰ noted that, if $p-1-\mu$ is the rank of the system (3) modulo p , the congruence, satisfied by the distinct roots $\neq 0$ of (2) and by these only, is given symbolically by

$$\left(\frac{\partial}{\partial a_1} x - \frac{\partial}{\partial a_0} \right)^\mu \mid a_{i+k} \mid \equiv 0 \pmod{p} \quad (i, k = 0, \dots, p-2).$$

He obtained easily Kronecker's²⁵ form of the last congruence. He gave necessary and sufficient conditions, expressed in terms of a complicated determinant and its $\mu-1$ successive derivatives with respect to a_{p-2} , in order that (2) and a second congruence of degree $p-2$ shall have μ common roots $\neq 0$, and found the congruence satisfied by these μ common roots. He deduced determinantal expressions for the sum σ_r of the r th powers of the roots of (2), and for the coefficients in terms of the σ 's.

Michael Demeczky³¹ would employ Euclid's process to find the g. c. d. $G(x)$ modulo p of (2) and $x^p - x$. If $G(x) \equiv 0 \pmod{p}$ is of degree ν it has ν real roots and these give all the real roots of (2). Multiple roots are then treated. The case of any composite modulus is known to reduce to the case of p^π , p a prime. If (2) has λ distinct real roots, not multiple roots, we can derive λ real roots of $f(x) \equiv 0 \pmod{p^\pi}$. If p_1, \dots, p_n are distinct primes and if $f(x) \equiv 0 \pmod{p_i}$ has λ_i real roots, then $f(x) \equiv 0 \pmod{p_1 \dots p_n}$ has $\lambda_1 \dots \lambda_n$ real roots, and is satisfied by every integer x if the former are. Various sets of necessary and sufficient conditions are found that $f(x) \equiv 0 \pmod{m = \prod p_i^{\pi_i}}$ shall have m distinct real roots; one set is that $f(x) \equiv 0 \pmod{p_i^{\pi_i}}$ identically for each i .

L. Gegenbauer³² proved that a congruence modulo p , a prime, of degree $p-2$ in each of n variables has a set of solutions each $\neq 0$ if and only if p divides the determinant of a cyclic matrix

$$\begin{pmatrix} A^0 & A^1 & \dots & A^{r-1} \\ A^{r-1} & A^0 & \dots & A^{r-2} \\ \dots & \dots & \dots & \dots \\ A^1 & A^2 & \dots & A^0 \end{pmatrix},$$

where A^μ is itself a cyclic matrix in B^0, \dots, B^{r-1} ; etc., until we reach matrices in the coefficients of the congruence. An upper limit is found for

²⁰Sitzungsber. Ak. Wiss. Wien (Math.), 98, IIa, 1889, 652-72.

³¹Math. u. Naturw. Berichte aus Ungarn, 8, 1889-90, 50-59. Math. és Termés Ertesítő, 7, 1889, 131-8.

³²Sitzungsber. Ak. Wiss. Wien (Math.), 99, IIa, 1890, 799-813.

the number of sets of solutions each not divisible by p . He proved that

$$\sum_{j=1}^s a_j x_j^{\frac{p-1}{2}} + \sum_{j=1}^n a_{s+j} x_{s+j} + b \equiv 0 \pmod{p}$$

has p^{n+s-1} sets of solutions. Of these,

$$\frac{1}{p} \left(\frac{p-1}{2} \right)^s \{ 2^r [(p-1)^n - (-1)^n] - (-1)^{n-1} pr \}$$

have each $x \not\equiv 0$, where r is the number of the 2^s integers

$$b \pm a_1 \pm a_2 \pm \dots \pm a_s$$

which are divisible by p . The number of sets of solutions of

$$\sum_{j=1}^s a_j x_j^{\frac{p-1}{2}} + \sum_{j=1}^n a_{s+j} x_{s+j}^2 + b \equiv 0 \pmod{p}$$

is expressed in terms of the functions used for quadratic congruences.

*E. Snopek³³ gave a generalization of König's criterion for the solvability of a congruence modulo p .

L. Gegenbauer³⁴ proved that if the ρ congruences

$$\sum_{k=0}^{p-2} z_{k\lambda} x^{p-2-k} \equiv 0 \pmod{p} \quad (\lambda = 0, 1, \dots, \rho-1)$$

have in common at least $p-\rho$ distinct roots not divisible by p then all ρ -rowed determinants in the matrix $(z_{k\lambda})$ are divisible by p . The converse is proved when a certain condition holds. By specialization, König's theorem is obtained.

Gegenbauer³⁵ proved that, if r is less than the prime p and if z_0, \dots, z_{r-1} are incongruent and not divisible by p , the system of linear congruences

$$(4) \quad \sum_{k=0}^{p-2} b_{k+\rho} y_k \equiv 0 \pmod{p} \quad (\rho = 0, 1, \dots, p-2)$$

has all its sets of solutions of the form

$$(5) \quad y_k \equiv \sum_{\lambda=0}^{r-1} a_r z_\lambda^k \quad (k = 0, 1, \dots, p-2)$$

or not, according as the matrix $(b_{k+\rho})$, $k = r, r+1, \dots, p-2$; $\rho = 0, \dots, p-2$, has a $p-r-1$ rowed determinant prime to p or not. Next, if

$$(6) \quad \sum_{k=0}^{p-2} b_k x^k \equiv 0 \pmod{p}$$

has exactly r distinct roots z_0, \dots, z_{r-1} each not divisible by p , every system of solutions of (4) is given by (5), and conversely. By combining this theorem of Kronecker's with the former, we obtain Kronecker's form of König's theorem.

³³Prace Mat. Fiz., Warsaw, 4, 1893, 63-70 (in Polish).

³⁴Sitzungsber. Ak. Wiss. Wien (Math.), 102, IIa, 1893, 549-64.

³⁵Monatshefte Math. Phys., 5, 1894, 230-2. Cf. Gegenbauer.²⁸

K. Zsigmondy³⁶ proved that, if p is a prime, there are exactly

$$\psi(n, k) = p^n - \binom{k}{1} p^{n-1} + \binom{k}{2} p^{n-2} - \dots + (-1)^n \binom{k}{n}$$

congruences $x^n + \dots \equiv 0 \pmod{p}$ not having as roots k given distinct numbers. Also,

$$\psi(n, k) = p\psi(n-1, k) + (-1)^n \binom{k}{n}, \quad \psi(n, k+1) = \psi(n, k) - \psi(n-1, k).$$

If $n \geq k$, $\psi(n, k) = p^{n-k}(p-1)^k$. For $n=k$, $\psi(n, k)$ is the number $\psi(n)$ of congruences of degree n with no root. The number with exactly i roots is $\binom{p}{i}\psi(n-i)$. There are $\binom{p-1}{i}\psi(i-r)$ distinct matrices (3) of rank i such that a_{r-1} is the first one of a_0, a_1, \dots not divisible by p .

K. Zsigmondy³⁷ considered a function $\Phi(f)$ of a polynomial $f(x)$ such that Φ is unaltered when the coefficients of $f(x)$ are increased by integral multiples of the prime p . Let $f_k^{(i)}(x)$, $i=1, \dots, p^k$, denote the polynomials of degree k which are distinct modulo p and have unity as the coefficient of x^k . It is stated that

$$\begin{aligned} \sum_a \Phi\{f_n^{(a)}(x)\} &= \sum_{j=1}^{p^n} \Phi\{f_n^{(j)}(x)\} - \sum_i \sum_{j=1}^{p^{n-1}} \Phi\{(x-a_i)f_{n-1}^{(j)}(x)\} \\ &\quad + \sum_{i, i'} \sum_{j=1}^{p^{n-2}} \Phi\{(x-a_i)(x-a_{i'})f_{n-2}^{(j)}(x)\} - \dots, \end{aligned}$$

where a takes those values $1, 2, \dots, p^n$ for which $f_n^{(a)}(x) \equiv 0 \pmod{p}$ does not have as a root one of the given incongruent numbers a_1, \dots, a_s ; while, in the outer sums on the right, i, i', \dots range over the combinations of $1, \dots, s$ without repetitions.

Zsigmondy³⁸ had earlier given the preceding formula for the case in which a_1, \dots, a_s denote $0, 1, \dots, p-1$. Then taking $\Phi(f)=1$, we get the number of congruences of degree n with no root (Zsigmondy³⁶). Taking $\Phi(f)=f$, we see that the sum of the congruences of degree n with no root is $\equiv 0 \pmod{p}$, aside from specified exceptions. Taking $\Phi(f)=\omega'$, where ω is a p th root of unity, and $n \geq p$, we see that the system $f_n^{(a)}(x)$ takes each of the values $1, \dots, p-1 \pmod{p}$ equally often.

Zsigmondy³⁹ proved his^{36, 37} earlier formulas, obtained for an integral value of x the number of complete sets of residues modulo p into which fall the values of the $f_n^{(a)}(x)$ not having prescribed roots, and investigated the system B_n of the least positive residues modulo p of the left members of all congruences of degree n having no root. In particular, he found how often the system B_n contains each residue, or non-residue, of a q th power. He investigated (pp. 19-36) the number of polynomials in x which take k prescribed residues modulo p for k given values of x .

³⁶Sitzungsber. Ak. Wiss. Wien (Math.), 103, IIa, 1894, 135-144.

³⁷Monatshefte Math. Phys., 7, 1896, 192-3.

³⁸Jahresbericht d. Deutschen Math. Verein., 4, 1894-5, 109-111.

³⁹Monatshefte Math. Phys., 8, 1897, 1-42.

L. Gegenbauer⁴⁰ proved that (2) has as a root a quadratic residue or non-residue of the prime p if and only if the respective determinant

$$P = | a_{\mu+i} + a_{\mu+i+\pi} |, \quad N = | a_{\mu+i} - a_{\mu+i+\pi} | \quad (i, \mu = 0, \dots, \pi-1)$$

be divisible by p , where $\pi = (p-1)/2$. From this it is proved that (2) has exactly $\pi-r$ distinct quadratic residues (or non-residues) of p as roots if and only if P (or N) and its $\pi-1-r$ successive derivatives with respect to $a_{\pi-1} + a_{p-2}$ have the factor p , while the derivative of order $\pi-r$ is prime to p . These residues satisfy the congruence

$$\left\{ x \frac{\partial}{\partial(a_1 + a_{\pi+1})} - \frac{\partial}{\partial(a_0 + a_{\pi})} \right\}^{(\pi-r)} K \equiv 0 \pmod{p},$$

where $K = P$ or N , while the ν th power of the sign of differentiation represents the ν th derivative. A second set of conditions is obtained. Congruence (2) has exactly $\pi-1-\kappa$ distinct quadratic residues as roots if and only if the determinants of type P with now $i=0, \dots, \kappa, \kappa+1$ and $\mu=0, \dots, \kappa, \tau$, are divisible by p for $\tau=\kappa+1, \dots, \pi-1$; while p is not a factor of the determinant of type P with now $i, \mu=0, \dots, \kappa$. These residues are the roots of

$$\sum_{\tau=\kappa}^{\pi} | a_{\mu+i} + a_{\mu+i+\tau} | x^{\pi-1-\tau} \equiv 0 \pmod{p},$$

where $i=0, \dots, \kappa$, and $\mu=0, \dots, \kappa-1, \tau$ in the determinants. For non-residues w_e have only to use the differences of a 's in place of sums.

S. O. Satunovskij⁴¹ noted that, for a prime modulus p , a congruence of degree n ($n < p$) has n distinct roots if and only if its discriminant is not divisible by p and $S_{p+q} \equiv S_{q+1} \pmod{p}$ for $q=1, \dots, n-1$, where S_k is the sum of the k th powers of the n roots.

A. Hurwitz⁴² gave an expression for the number N of real roots of

$$f(x) = a_0 + a_1x + \dots + a_rx^r \equiv 0 \pmod{p},$$

where p is a prime. By Fermat's theorem,

$$N \equiv \sum_{x=1}^{p-1} \{1 - f(x)^{p-1}\} \pmod{p}.$$

Let $f(x)^{p-1} = C_0 + C_1x + \dots$. Then N is determined by

$$N+1 \equiv C_0 + C_{p-1} + C_{2(p-1)} + \dots \pmod{p}.$$

Let $f(x_1, x_2)$ be the homogeneous form of $f(x)$. Let A be the number of sets of solutions of $f(x_1, x_2) \equiv 0 \pmod{p}$, regarding (x_1, x_2) and (x_1', x_2') as the same solution if $x_1' \equiv \rho x_1, x_2' \equiv \rho x_2 \pmod{p}$ for an integer ρ . Then

$$A-1 \equiv -a_0^{p-1} - a_r^{p-1} + \sum \frac{(p-1)!}{a_0! \dots a_r!} a_0^{a_0} \dots a_r^{a_r} \pmod{p},$$

⁴⁰Sitzungsber. Ak. Wiss. Wien (Math.), 110, IIa, 1901, 140-7.

⁴¹Kazan' Izv. fiz. mat. Obsc. (Math. Soc. Kasan), (2), 12, 1902, No. 3, 33-49. Zap. mat. otd. Obsc., 20, 1902, I-II.

⁴²Archiv Math. Phys., (3), 5, 1903, 17-27.

where the summation extends over the sets of solutions ≥ 0 of

$$a_0 + a_1 + \dots + a_r = p - 1, \quad a_1 + 2a_2 + \dots + ra_r \equiv 0 \pmod{p-1}.$$

The right member is an invariant modulo p of $f(x_1, x_2)$ with respect to all linear homogeneous transformations on x_1, x_2 with integral coefficients whose determinant is not divisible by p . The final sum in the expression for $A - 1$ is congruent to $N + 1$. If $r = 2$, $p > 2$, the invariant is congruent to the power $(p-1)/2$ of the discriminant $a_1^2 - 4a_0a_2$ of f .

*E. Stephan⁴³ investigated the number of roots of linear congruences and systems of congruences.

H. Kühne⁴⁴ considered $f(x) = x^m + \dots + a_m$ with no multiple irreducible factor and with a_m not a multiple of the prime p . For $n < m$, let $g = x^n + \dots + b_n$ have arbitrary coefficients. The resultant $R(f, g)$ is zero modulo p if and only if f and g have a common factor modulo p . Thus the number of all g 's of degree n which have no common factor with f modulo p is ρ_n , where

$$\rho_n \equiv \sum \{R(f, g)\}^\omega \pmod{p^n}, \quad \omega = p^{n-1}(p-1),$$

the summation extending over the p^n possible g 's. He expressed ρ_n as a sum of binomial coefficients. For any two binary forms ϕ, ψ of degrees m, n , it is shown that

$$J_n = \sum_{\downarrow} \{R(\phi, \psi)\}^\omega$$

is invariant modulo p^n under linear transformations with integral coefficients of determinant prime to p ; J_1 is Hurwitz's⁴² invariant.

M. Cipolla⁴⁵ used the method of Hurwitz⁴² to find the sum of the k th powers of the roots of a congruence, and extended the method to show that the number of common roots of $f(x) \equiv 0, g(x) \equiv 0 \pmod{p}$, of degrees r, s , is congruent to $-\sum C_j K_i$, where i, j take the values for which

$$0 < i \leq s(p-1), \quad 0 < j \leq r(p-1), \quad i+j \equiv 0 \pmod{p},$$

the C 's being as with Hurwitz, and similarly

$$g(x)^{p-1} = K_0 + K_1x + \dots$$

The number of roots common to n congruences is given by a sum.

L. E. Dickson⁴⁶ gave a two-fold generalization of Hurwitz's⁴² formula for the number of integral roots of $f(x) \equiv 0 \pmod{p}$. The first generalization is to the residue modulo p of the number of roots which are rational in a root of an irreducible congruence of a given degree. A further generalization is obtained by taking the coefficients a_i of $f(x)$ to be elements in the Galois field of order p^n (cf. Galois⁶², etc.). Then let N be the number of roots of $f(x) = 0$ which belong to the Galois field of order $P = p^{nm}$. Then

⁴³Jahresber. Staatsoberrrealsch. Steyer, 34, 1903-4, 3-40.

⁴⁴Archiv Math. Phys., (3), 6, 1904, 174-6.

⁴⁵Periodico di Mat., 22, 1907, 36-41.

⁴⁶Bull. Amer. Math. Soc., 14, 1907-8, 313.

$N \equiv N^* \pmod{p}$, where $N^* + 1$ is derived from either of Hurwitz's two sums for $N + 1$ by replacing p by P . The same replacement in Hurwitz's expression for $A - 1$ leads to the invariant $A^* - 1$, where A^* is congruent modulo p to the number of distinct sets of solutions in the Galois field of order p^m of the equation $f(x_1, x_2) = 0$.

G. Rados⁴⁷ considered the sets of solutions of

$$f(x, y) = \sum_{k=0}^{p-2} (a_0^{(k)} x^{p-2} + a_1^{(k)} x^{p-3} + \dots + a_{p-2}^{(k)}) y^{p-k-2} \equiv 0 \pmod{p}$$

for a prime p . Let A_k denote the matrix of D , in (3), with a_i replaced by $a_i^{(k)}$. Let C denote the determinant of order $(p-1)^2$ obtained from D by replacing a_k by matrix A_k . Then $f \equiv 0$ has a solution other than $x \equiv y \equiv 0$ if and only if C is divisible by p ; it has exactly r sets of solutions other than $x \equiv y \equiv 0$ if and only if C is of rank $(p-1)^2 - r$.

To obtain theorems including the possible solution $x \equiv y \equiv 0$, use

$$\phi(x, y) = \sum_{k=0}^{p-1} (a_0^{(k)} x^{p-1} + a_1^{(k)} x^{p-2} + \dots + a_{p-1}^{(k)}) y^{p-k-1} \equiv 0 \pmod{p},$$

$$\alpha = \begin{pmatrix} a_0 & a_1 & \dots & a_{p-3} & a_{p-2} & a_{p-1} \\ a_1 & a_2 & \dots & a_{p-2} & a_{p-1} + a_0 & 0 \\ a_2 & a_3 & \dots & a_{p-1} + a_0 & a_1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{p-1} + a_0 & a_1 & \dots & a_{p-3} & a_{p-2} & 0 \end{pmatrix},$$

and α_k derived from α by replacing a_i by $a_i^{(k)}$. Let γ be the determinant derived from $|\alpha|$ by replacing a_k by matrix α_k and 0 by a matrix whose p^2 elements are zeros. Then $\phi \equiv 0$ has a set of real solutions if and only if $\gamma \equiv 0 \pmod{p}$; it has r sets of solutions if and only if γ is of rank $p^2 - r$.

*P. B. Schwacha⁴⁸ discussed the number of roots of congruences.

*G. Rados⁴⁹ treated higher congruences.

THEORY OF HIGHER CONGRUENCES, GALOIS IMAGINARIES.

C. F. Gauss,⁶⁰ in a posthumous paper, remarked that "the solution of congruences is only a part of a much higher investigation, viz., that of the factorization of functions modulo p . Even when $\xi(x) \equiv 0$ has no real root, ξ may be a product of factors of degrees ≥ 2 , each of which could be said to have imaginary roots. If use had been made of a similar freedom which younger mathematicians have permitted themselves, and such imaginary roots had been introduced, the following investigation could be greatly condensed." As the later work of Serret⁴⁴ shows, such imaginaries can be

⁴⁷Ann. Sc. École Normale Sup., (3), 27, 1910, 217-231. Math. és Termés. Értesítő (Report of Hungarian Ac.), Budapest, 27, 1909, 255-272.

⁴⁸Ueber die Existenz und Anzahl der Wurzeln der Kongruenz $\sum c_i x^i \equiv 0 \pmod{m}$, Progr. Wilhering, 1911, 30 pp.

⁴⁹Math. és Termés. Értesítő, Budapest, 29, 1911, 810-826.

⁶⁰Werke, 2, 1863, 212-240. Maser's German translation of Gauss' Disq. Arith., etc., 1889, 604-629.

introduced in a way free from any logical objections. Avoiding their use, Gauss began his investigation by showing that two polynomials in x with integral coefficients have a greatest common divisor modulo p , which can be found by Euclid's process. It is understood throughout that p is a prime (cf. Maser, p. 627). Hence if A and B are relatively prime polynomials modulo p , there exist two polynomials P and Q such that

$$PA + QB \equiv 1 \pmod{p}.$$

Thus if A has no factor in common with B or C modulo p , we find by multiplying the preceding congruence by C that A has no factor in common with the product BC modulo p . If a polynomial is divisible by A, B, C, \dots , no two of which have a common factor modulo p , it is divisible by their product.

A polynomial is called prime modulo p if it has no factor of lower degree modulo p . Any polynomial is either prime or is expressible in a single way as a product of prime polynomials modulo p . The number of distinct polynomials $x^n + ax^{n-1} + \dots$ modulo p is evidently p^n . Let (n) of these be prime functions. Then $p^n = \sum d(d)$, where d ranges over all the divisors of n (only a fragment of the proof is preserved). It is said to follow easily from this relation that, if n is a product of powers of the distinct primes a, b, \dots , then

$$n(n) = p^n - \sum p^{n/a} + \sum p^{n/ab} - \dots$$

The τ th powers of the roots of an equation $P=0$ with integral coefficients are the roots of an equation $P_\tau=0$ of the same degree with integral coefficients. If τ is a prime, $P_\tau \equiv P \pmod{\tau}$.

A prime function P of degree m , other than x itself, divides $x^m - 1$ for some value of $\nu < p^m$. If ν is the least such integer, ν is a divisor of $p^m - 1$. Hence P divides

$$(1) \quad x^{p^m-1} - 1.$$

The latter is congruent modulo p to the product of the prime functions, other than x , whose degrees are the various divisors of m .

If $P = x^m - Ax^{m-1} + Bx^{m-2} - \dots$ is a prime function modulo p , the remainders by dividing the sum, the sum of the products by twos, etc., of

$$x, x^p, x^{p^2}, \dots, x^{p^{m-1}}$$

by P are congruent to A, B , etc., respectively.

If ν is not divisible by p and if m is the least positive integer for which $p^m \equiv 1 \pmod{\nu}$, each prime function dividing $x^m - 1$ modulo p is a divisor of (1) and its degree is therefore a divisor of m . Let δ be a divisor of m , and δ', δ'', \dots the divisors $< \delta$ of δ ; let μ be the g. c. d. of ν and $p^\delta - 1$, μ' the g. c. d. of ν and $p^{\delta'} - 1$, \dots and set $\lambda' = \mu/\mu'$, $\lambda'' = \mu/\mu''$, \dots . Then the number of prime divisors modulo p of degree δ of $x^m - 1$ is N/δ , if N is the number of integers $< \mu$ which are divisible by no one of $\lambda', \lambda'', \dots$. A method of finding all prime functions dividing $x^m - 1$ is based on periods of powers of x with exponents $< \nu$ and prime to ν (pp. 620-2).

If X has been expressed as a product of relatively prime factors modulo p , we can express X as a product of a like number of factors mod p^n congruent to the former factors modulo p . There is a fragment on the case of multiple factors.

C. G. J. Jacobi⁶¹ noted that, if q is a prime $6n-1$, $x^{q+1} \equiv 1 \pmod{q}$ has $q-1$ imaginary roots $a+b\sqrt{-3}$, where $a+3b^2 \equiv 1 \pmod{q}$, besides the roots ± 1 .

E. Galois⁶² employed imaginary roots of any irreducible congruence $F(x) \equiv 0 \pmod{p}$, where p is a prime. Let i be one imaginary root of this congruence of degree ν . Let a be one of the $p^\nu-1$ expressions

$$a + a_1 i + a_2 i^2 + \dots + a_{\nu-1} i^{\nu-1}$$

in which the a 's are integers $< p$, not all zero. Since each power of a can be expressed as such a polynomial, we have $a^n = 1$ for some positive integer n . Let n be a minimum. Then $1, a, \dots, a^{n-1}$ are distinct. Multiply them by a new polynomial β in i ; we get n products distinct from each other and from the preceding powers of a . If $2n < p^\nu - 1$, we use a new multiplier, etc. Hence n divides $p^\nu - 1$, and

$$(2) \quad a^{p^\nu-1} = 1.$$

[This is known as Galois's generalization of Fermat's theorem.] It follows that there exist primitive roots a such that $a^e \neq 1$ if $e < p^\nu - 1$. Any primitive root satisfies a congruence of degree ν irreducible modulo p .

Every irreducible function $\tilde{F}(x)$ of degree ν divides $x^{p^\nu} - x$ modulo p . Since $\{F(x)\}^{p^n} \equiv F(x^{p^n})$ modulo p , the roots of $F(x) \equiv 0$ are

$$i, i^p, i^{p^2}, \dots, i^{p^{\nu-1}}.$$

All the roots of $x^{p^\nu} = x$ are polynomials in a certain root i , which satisfies an irreducible congruence of degree ν . To find all irreducible congruences of degree ν modulo p , delete from $x^{p^\nu} - x$ all factors which it has in common with $x^{p^\mu} - x$, $\mu < \nu$. The resulting congruence is the product of the desired ones; the factors may be obtained by the method of Gauss, since each of their roots is expressible in terms of a single root. In practice, we find by trial one irreducible congruence of degree ν , and then a primitive root of (2); this is done for $p=7$, $\nu=3$.

Any congruence of degree n has n real or imaginary roots. To find them, we may assume that there is no multiple root. The integral roots are found from the g. c. d. of $F(x)$ and $x^{p-1} - 1$. The imaginary roots of the second degree are found from the g. c. d. of $F(x)$ and $x^{p^2-1} - 1$; etc.

V. A. Lebesgue⁶³ noted that, if p is a prime, the roots of all quadratic

⁶¹Jour. für Math., 2, 1827, 67; Werke, 6, 235.

⁶²Sur la théorie des nombres, Bulletin des Sciences Mathématiques de M. Férussac, 13, 1830, 428. Reprinted in Jour. de Mathématiques, 11, 1846, 381; Oeuvres Math. d'Evariste Galois, Paris, 1897, 15-23; Abhand. Alg. Gleich. Abel u. Galois, Maser, 1889, 100.

⁶³Jour. de Mathématiques, 4, 1839, 9-12.

congruences modulo p are of the form $a + b\sqrt{n}$, where n is a fixed quadratic non-residue of p , while a, b are integers. But the cube root of a non-cubic residue is not reducible to this form $a + b\sqrt{n}$. The $p+1$ sets of integral solutions of $y^2 - nz^2 \equiv a \pmod{p}$ yield the $p+1$ real or imaginary roots $x = y + z\sqrt{n}$ of $x^{p+1} \equiv a \pmod{p}$. The latter congruence has primitive roots if $a = 1$.

Th. Schönemann⁶⁴ built a theory of congruences without the use of Euclid's g. c. d. process. He began with a proof by induction that if a function is irreducible modulo p and divides a product AB modulo p , it divides A or B . Much use is made of the concept norm Nf_ϕ of $f(x)$ with respect to $\phi(x)$, i. e., the product $f(\beta_1) \dots f(\beta_m)$, where β_1, \dots, β_m are the roots of $\phi(x) = 0$; the norm is thus essentially the resultant of f and ϕ . The norm of an irreducible function with respect to a function of lower degree is shown by induction to be not divisible by p . Hence if f is irreducible and $Nf_\phi \equiv 0 \pmod{p}$, then f is a divisor of ϕ modulo p . A long discussion shows that if $\alpha_1, \dots, \alpha_n$ are the roots of an algebraic equation $f(x) = x^n + \dots = 0$ and if $f(x)$ is irreducible modulo p , then $\prod_{i=1}^n \{z - \phi(\alpha_i)\}$ is a power of an irreducible function modulo p .

If α is a root of $f(x)$ and $f(x)$ is irreducible modulo p , and if $\phi(\alpha) = \psi(\alpha) + pR(\alpha)$, we write $\phi \equiv \psi \pmod{p, \alpha}$; then $\phi(x) - \psi(x)$ is divisible by $f(x)$ modulo p . If the product of two functions of α is $\equiv 0 \pmod{p, \alpha}$, one of the functions is $\equiv 0$.

If $f(x) = x^n + \dots$ is irreducible modulo p and if $f(\alpha) = 0$, then

$$f(x) \equiv (x - \alpha)(x - \alpha^p) \dots (x - \alpha^{p^{n-1}}), \quad \alpha^{p^n - 1} \equiv 1 \pmod{p, \alpha},$$

$$x^{p^n - 1} - 1 = \prod_{i=1}^{p^n - 1} \{x - \phi_i(\alpha)\} \pmod{p, \alpha},$$

where ϕ_i is a polynomial of degree $n-1$ in α with coefficients chosen from $0, 1, \dots, p-1$, such that not all are zero. There exist $\phi(p^n - 1)$ primitive roots modulus p, α , i. e., functions of α belonging to the exponent $p^n - 1$.

Let $F(x)$ be irreducible modulus p, α , i. e., have no divisor of degree ≥ 1 modulus p, α . Let $F(\beta) = 0$, algebraically. Two functions of β with coefficients involving α are called congruent modulus p, α, β if their difference is the product of p by a polynomial in α, β . It is proved that

$$F(x) \equiv (x - \beta)(x - \beta^p) \dots (x - \beta^{p^{(m-1)n}}), \quad \beta^{p^{mn}} \equiv 1 \pmod{p, \alpha, \beta}.$$

If $\nu < n$, n being the degree of $f(x)$, and if the function whose roots are the $(p^\nu - 1)$ th powers of the roots of $f(x)$ is $\not\equiv 0 \pmod{p}$ for $x = 1$, then $f(x)$ is irreducible modulo p . Hence if m is a divisor of $p - 1$ and if g is a primitive root of p , and if k is prime to m , then $x^m - g^k$ is irreducible modulo p .

If $\nu < m$, m being the degree of $F(x)$, and if the function whose roots are the $(p^\nu - 1)$ th powers of the roots of $F(x)$ is $\not\equiv 0 \pmod{p, \alpha}$ for $x = 1$, then

⁶⁴Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, Progr., Brandenburg, 1844. Same in Jour. für Math., 31, 1846, 269-325.

$F(x)$ is irreducible modulus p, a . Hence if m is a divisor of $p^n - 1$, and if $g(a)$ is a primitive root of

$$x^{p^n-1} \equiv 1 \pmod{p, a},$$

and if k is prime to m , then $x^m - g^k$ is irreducible modulus p, a .

If $F(x, a)$ is irreducible modulus p, a , and if at least one coefficient satisfies

$$x^{p^\nu-1} \equiv 1 \pmod{p, a}$$

if and only if ν is a multiple of n , then

$$\psi(x) \equiv \prod_{j=0}^{n-1} F(x, a^{p^j}) \pmod{p, a}$$

has integral coefficients and is irreducible modulo p .

If $G(x)$ is of degree mn and is irreducible modulo p , and $G(a) = 0$, algebraically, and if $r(a)$ is a primitive root of $x^{p^{mn}} \equiv 1 \pmod{p, a}$, then

$$\chi(x) \equiv \prod_{j=0}^{m-1} (x - t^{p^j}), \quad t = r^e, \quad e = \frac{p^{mn} - 1}{p^m - 1},$$

has integral coefficients and is irreducible modulo p .

The last two theorems enable us to prove the existence of irreducible congruences modulo p of any degree. First,

$$(x^{p^{p^n-1}} - 1) / (x^{p^{p^n-1}-1} - 1)$$

is the product of the irreducible functions of degree p^n modulo p . To prove the existence of an irreducible function of degree lp^n , where l is any integer prime to p , assume that there exists an irreducible function of each degree $< lp^n$, and hence for the degree $a = Ap^n$, where $A = \phi(l) < l$. Let a be a root of the latter, and r a primitive root of $x^{P-1} \equiv 1 \pmod{p, a}$, where $P = p^a$. Since l divides $P - 1$ by Euler's generalization of Fermat's theorem, $x^l - r$ is irreducible modulus p, a . Hence by the theorem preceding the last, $\prod_{j=0}^{A-1} (x^l - r^{p^j})$ is irreducible modulo p . Since its degree is $lp^n A$, the last theorem gives an irreducible congruence of degree lp^n .

Every irreducible factor modulo p of $x^{p^n-1} - 1$ is of degree a divisor of n . Conversely, every irreducible function of degree a divisor of n is a factor of that binomial. If n is a prime, the number of irreducible functions modulo p of degree n is $(p^{p^n} - p^{p^n-1})/n$. If n is a product of powers of distinct primes A, B, \dots , say four, the number of irreducible congruences of degree n modulo p is

$$\frac{1}{n} \{ P^{ABCD} - P^{ABC} - \dots - P^{BCD} + P^{AB} + \dots + P^{CD} - P^A - \dots - P^D \},$$

where $P = p^{n/(ABCD)}$. Replacing p by p^m , we get the number of irreducible congruences of degree n modulus p, a , where a is a root of an irreducible congruence of degree m .

If n is a prime and p belongs to the exponent e modulo n , $f = (x^n - 1)/(x - 1)$ is congruent modulo p to the product of $(n-1)/e$ irreducible functions of

degree e modulo p . Hence if p is a primitive root of n , f is irreducible modulo p , and therefore with respect to each of the infinitude of primes $p + \gamma n$. Thus f is algebraically irreducible.

Schönemann⁶⁵ considered congruences modulo p^m . If $g(x)$ is not divisible by p , and $f = x^n + \dots$ is irreducible modulo p^m and if $A(x)$ is not divisible by f modulo p , then $fg \equiv AB \pmod{p^m}$ implies that $B(x)$ is divisible by f modulo p^m . If $f \equiv f_1, g \equiv g_1 \pmod{p}$ and the leading coefficients of the four functions are unity, while f and g have no common factor modulo p , then $fg \equiv f_1 g_1 \pmod{p^m}$ implies $f \equiv f_1, g \equiv g_1 \pmod{p^m}$. He proved the final theorem of Gauss.⁶⁶ Next, $(x-a)^n + pF(x)$ is irreducible modulo p^2 if and only if $F(a) \not\equiv 0 \pmod{p}$; an example is

$$\frac{x^p - 1}{x - 1} = (x - 1)^{p-1} + pF(x), \quad F(1) = 1.$$

Henceforth, let $f(x)$ be irreducible modulo p and of degree n . If $f(x)^n + pF(x)$ is reducible modulo p^2 , then (p. 101) $f(x)$ is a factor of $F(x)$ modulo p . If $f(a) = 0$ and $g(a) \not\equiv 0 \pmod{p, a}$, then $g^e \equiv 1 \pmod{p^m, a}$, where $e = p^{m-1}(p^n - 1)$. If the roots of $G(z)$ are the (p^{m-1}) th powers of the roots of $f(x)$, then

$$G(z) \equiv (z - \beta)(z - \beta^p) \dots (z - \beta^{p^{n-1}}) \pmod{p^m, a}.$$

If M is any integer and if $F(x)$ has the leading coefficient unity, we can find z and w such that $(x^2 - 1)^w$ is divisible by $F(x)$ modulo M .

A. Cauchy⁶⁶ noted the uniqueness of the factorization of a function $f(x)$ with integral coefficients into irreducible factors modulo p , a prime. An irreducible function divides a product only when it divides one factor modulo p . A common divisor of two functions divides their g. c. d. modulo p .

Cauchy⁶⁷ employed an indeterminate quantity or symbol i and defined $f(i)$ to be not the value of the polynomial $f(x)$ for $x = i$, but to be $a + bi$ if $a + bx$ is the remainder obtained by dividing $f(x)$ by $x^2 + 1$. In particular, if $f(x)$ is $x^2 + 1$ itself, we have $i^2 + 1 = 0$.

Similarly, if $\omega(x) \equiv 0$ is an irreducible congruence modulo p , a prime, let i denote a symbolic root. Then $\phi(i)\psi(i) \equiv 0$ implies either $\phi(i) \equiv 0$ or $\psi(i) \equiv 0 \pmod{p}$. At most n integral functions of i satisfy $f(x, i) \equiv 0 \pmod{p}$, if the degree of f in x is $n < p$. If our $\omega(x)$ divides $x^n - 1$, but not $x^m - 1$, $m < n$, modulo p , where n is not a divisor of $p - 1$, call i a symbolic primitive root of $x^n \equiv 1 \pmod{p}$. Then $x^n - 1 \equiv (x - 1)(x - i) \dots (x - i^{n-1})$. If s is a primitive root of n and if $n - 1 = gh$, and $p^g \equiv 1 \pmod{n}$,

$$\prod_{j=0}^{g-1} (x - i^{s^{k+jh}})$$

equals a function of x with integral coefficients, while every factor of $x^n - 1$ modulo p with integral coefficients equals such a product.

⁶⁵Jour. für Math., 32, 1846, 93-105.

⁶⁶Comptes Rendus Paris, 24, 1847, 1117; Oeuvres, (1), 10, 308-12.

⁶⁷Comptes Rendus Paris, 24, 1847, 1120; Oeuvres, (1), 10, 312-23.

G. Eisenstein⁶⁸ stated that if $f(x) \equiv 0$ is irreducible modulo p , and a is a root of the equation $f(x) = 0$ of degree n , and if a_0, a_1, \dots are any integers,

$$K = a_0 + a_1 a + \dots + a_{n-1} a^{n-1}$$

is congruent modulus p, a to one and but one expression

$$B = b_0 \beta + b_1 \beta^p + b_2 \beta^{p^2} + \dots + b_{n-1} \beta^{p^{n-1}},$$

where the b 's are integers and β is a suitably chosen function of a . Hence the p^n numbers B form a complete set of residues modulus p, a . If ω is a primitive n th root of unity, and if

$$\phi(\lambda) = a + \omega^\lambda a^p + \omega^{2\lambda} a^{p^2} + \dots + \omega^{(n-1)\lambda} a^{p^{n-1}},$$

the product $\phi(\lambda)\phi(\lambda') \dots$ is independent of a if $\lambda + \lambda' + \dots$ is divisible by n .

Th. Schönemann⁶⁹ proved the last statement in case n is not divisible by p . To make $K = B$, raise it to the powers p, p^2, \dots, p^{n-1} and reduce by $\beta^{p^n} \equiv \beta \pmod{p, a}$. This system of n congruences determines β uniquely if the cyclic determinant of order n with the elements b_i is not divisible by p ; in the contrary case there may not exist a β . The statement that the expressions B form p^n distinct residues is false if β is a root of a congruence of degree $< n$ irreducible modulo p ; it is true if β is a root of such a congruence of degree n and if

$$\beta + \beta^p + \dots + \beta^{p^{n-1}} \not\equiv 0 \pmod{p, a}.$$

J. A. Serret⁷⁰ made use of the g. c. d. process to prove that if an irreducible function $F(x)$ divides a product modulo p, a prime, it divides one factor modulo p . Then, following Galois, he introduced an imaginary quantity i verifying the congruence $F(i) \equiv 0 \pmod{p}$ of degree $\nu > 1$, but gave no formal justification of their use, such as he gave in his later writings. However, he recognized the interpretation that may be given to results obtained from their use. For example, after proving that any polynomial $a(i)$ with integral coefficients is a root of $a^{p^\nu} \equiv a \pmod{p}$, he noted that this result, for the case $a = i$, may be translated into the following theorem, free from the consideration of imaginaries: If $F(x)$ is of degree ν , has integral coefficients, and is irreducible modulo p , there exist polynomials $f(x)$ and $\chi(x)$ with integral coefficients such that

$$x^{p^\nu} - x = f(x)F(x) + p\chi(x).$$

The existence of an irreducible congruence of any given degree and any prime modulus is called the chief theorem of the subject. After remarking that Galois had given no satisfactory proof, Serret gave a simple and ingenious argument; but as he made use of imaginary roots of congruences without giving an adequate basis to their theory, the proof is not conclusive.

⁶⁸Jour. für Math., 39, 1850, 182.

⁶⁹Jour. für Math., 40, 1850, 185-7.

⁷⁰Cours d'algèbre supérieure, ed. 2, Paris, 1854, 343-370.

R. Dedekind⁷¹ developed the subject of higher congruences by the methods of elementary number theory without the use of algebraic principles. As by Gauss⁶⁰ he developed the theory of the g. c. d. of functions modulo p , a prime, and their unique factorization into prime (or irreducible) functions, apart from integral factors. Two functions A and B are called congruent modulus p , M , if $A - B$ is divisible by the function M modulo p . We may add or multiply such congruences. If the g. c. d. of A and B is of degree d , $Ay \equiv B \pmod{p, M}$ has p^d incongruent roots $y(x)$ modulus p , M .

Let $\phi(M)$ denote the number of functions which are prime to M modulo p and are incongruent modulus p , M . Let μ be the degree of M . A primary function of degree α is one in which the coefficient of x^α is $\equiv 1 \pmod{p}$. If D ranges over the incongruent primary divisors of M , then $\sum \phi(D) = p^\mu$. If M and N are relatively prime modulo p , then $\phi(MN) = \phi(M)\phi(N)$. If A is a prime function of degree α , $\phi(A^\alpha) = p^{\alpha\alpha}(1 - 1/p^\alpha)$. If M is a product of powers of incongruent primary prime functions α, \dots, ρ ,

$$\phi(M) = p^\mu \left(1 - \frac{1}{p^\alpha}\right) \dots \left(1 - \frac{1}{p^\rho}\right).$$

If F is prime to M modulo p , $F^{\phi(M)} \equiv 1 \pmod{p, M}$, which is the generalization of Fermat's theorem. Hence if A is prime to M , the above linear congruence has the solution $y \equiv BA^{\phi(M)-1}$.

If P is a prime function of degree π , a congruence of degree n modulus p , P has at most n incongruent roots. Also

$$(3) \quad y^{p^\pi-1} - 1 \equiv \Pi(y - F) \pmod{p, P},$$

identically in y , where F ranges over a complete set of functions incongruent modulus p , P and not divisible by P . In particular, $1 + \Pi F \equiv 0 \pmod{p, P}$, the generalization of Wilson's theorem.

There are $\phi(p^\pi - 1)$ primitive roots modulus p , P . Hence we may employ indices in the usual manner, and obtain the condition for solutions of $y^n \equiv A \pmod{p, P}$, where A is not divisible by P . In particular, A is a quadratic residue or non-residue of P according as

$$A^{(p^\pi-1)/2} \equiv +1 \text{ or } -1 \pmod{p, P}.$$

His extension of the quadratic reciprocity law will be cited under that topic.

A function A belongs to the exponent ρ with respect to the prime function P of degree π if ρ is the least positive integer for which $A^{p^\rho} \equiv A \pmod{p, P}$. Evidently ρ is a divisor of π . Let $N(\rho)$ be the number of incongruent functions which belong to an exponent ρ which divides π . Then $p^\pi = \sum N(d)$, where d ranges over the divisors of π . By the principle of inversion (Ch. XIX),

$$N(\rho) = p^\rho - \sum p^{\rho/a} + \sum p^{\rho/ab} - \sum p^{\rho/abc} + \dots,$$

where a, b, \dots are the distinct primes dividing ρ . Since the quotient of this sum by its last term is not divisible by p , we have $N(\rho) > 0$.

⁷¹Jour. für Math., 54, 1857, 1-26.

The product of the incongruent primary prime functions modulo p whose degree divides π is congruent modulo p to

$$\{\pi\} = x^{p^\pi} - x.$$

Then, if $\psi(\rho)$ is the number of primary prime functions of any degree ρ , $\sum d\psi(d) = p^\pi$, where the summation extends over all divisors d of π . A comparison of this with $\sum N(d) = p^\rho$ above shows that $N(\rho) = \rho\psi(\rho)$. Another proof is based on the fact that

$$(y-A)(y-A^p)\dots(y-A^{p^{p-1}})$$

is congruent modulis p, P to a polynomial in y with integral coefficients which is a prime function. Moreover, if in (3) we associate the linear factors in which the F 's belong to the same exponent, we obtain a factor of the left member which is irreducible modulo p .

The product of the incongruent primary prime functions of degree m (m being divisible by no primes other than a, b, \dots) is congruent modulo p to

$$\frac{\{m\} \cdot \Pi \{m/ab\} \dots}{\Pi \{m/a\} \cdot \Pi \{m/abc\} \dots}.$$

H. J. S. Smith⁷² gave an exposition of the theory.

E. Mathieu,⁷³ in his famous paper on multiply transitive groups, gave without proof the factorization (p. 301; for $m=1$, p. 275)

$$h(z^{p^{mn}} - z) \equiv \Pi_a \{ (hz)^{p^{m(n-1)}} + (hz)^{p^{m(n-2)}} + \dots + (hz)^{p^m} + hz + a \},$$

where a ranges over the roots of $a^{p^m} \equiv a$, while $h^{p^{mn}} \equiv h$; and (p. 302; for $m=1$, p. 280)

$$h(z^{p^{mn}} - z) \equiv \Pi_\beta (h^{p^m} z^{p^m} - hz - \beta),$$

where β ranges over the roots of

$$z^{p^{m(n-1)}} + z^{p^{m(n-2)}} + \dots + z^{p^m} + z \equiv 0.$$

If Ω is a root of a congruence of degree n whose coefficients are roots of $z^{p^m} \equiv z$ and whose first member is prime to $z^{p^m} - z$, then (p. 303) all the roots of $z^{p^{mn}} \equiv z$ are given by $A_0 + A_1\Omega + \dots + A_{n-1}\Omega^{n-1}$, where the A 's satisfy $z^{p^m} \equiv z$.

J. A. Serret,⁷⁴ in contrast to his⁷⁰ earlier exposition, here avoided at the outset the use of Galois imaginaries. An irreducible function of degree ν modulo p divides $x^{p^\mu} - x$ modulo p if and only if ν divides μ . A simple

⁷²British Assoc. Reports, 1860, 120, §§69-71; Coll. M. Papers, 1, 149-155.

⁷³Jour. de Mathématiques, (2), 6, 1861, 241-323.

⁷⁴Mém. Ac. Sc. de l'Institut de France, 35, 1866, 617-688. Same in Cours d'algèbre supérieure, ed. 4, vol. 2, 1879, 122-189; ed. 5, 1885.

proof is given for Dedekind's⁷¹ final theorem on the product of all irreducible functions of degree m modulo p .

A function $F(x)$ of degree ν , irreducible modulo p , is said to belong to the exponent n if n is the least positive integer such that $x^n - 1$ is divisible by $F(x)$ modulo p . Then n is a divisor of $p^\nu - 1$, and a proper divisor of it, since it does not divide $p^\mu - 1$ for $\mu < \nu$. Let n be a product of powers of the distinct primes a, b, \dots . Then the product of all functions of degree ν , irreducible modulo p , which belong to an exponent n which is a proper divisor of $p^\nu - 1$, is congruent modulo p to

$$\frac{(x^n - 1) \cdot \Pi(x^{n/ab} - 1) \dots}{\Pi(x^{n/a} - 1) \cdot \Pi(x^{n/abc} - 1) \dots}$$

and their number is therefore $\phi(n)/\nu$.

By a skillful analysis, Serret obtained theorems of practical importance for the determination of irreducible congruences of given degrees. If we know the N irreducible functions of degree μ modulo p , which belong to the exponent $l = (p^\mu - 1)/d$, then if we replace x by x^λ , where λ is prime to d and has no prime factor different from those which divide $p^\mu - 1$, we obtain the N irreducible functions of degree $\lambda\mu$ which belong to the exponent λl , exception being made of the case when p is of the form $4h - 1$, μ is odd, and λ is divisible by 4. In this exceptional case, we may set $p = 2^i t - 1$, $i \geq 2$, t odd; $\lambda = 2^j s$, $j \geq 2$, s odd. Let k be the least of i, j . Then if we know the $N/2^{k-1}$ irreducible functions of odd degree μ modulo p which belong to the exponent l and if we replace x by x^λ , where λ is of the form indicated, is prime to d and contains only primes dividing $p^\mu - 1$, we obtain $N/2^{k-1}$ functions of degree $\lambda\mu$ each decomposable into 2^{k-1} irreducible factors, thus giving N irreducible functions of degree $\lambda\mu/2^{k-1}$ which belong to the exponent λl . Apply these theorems to $x - g^e$, which belongs to the exponent $(p - 1)/d$ if g is a primitive root of p and if d is the g. c. d. of e and $p - 1$; we see that $x^\lambda - g^e$ is irreducible unless the exceptional case arises, and is then a product of 2^{k-1} irreducible functions. In that case, irreducible trinomials of degree λ are found by decomposing $x^\nu - g^e$, where $\nu = 2^{i-1}\lambda$.

If a is not divisible by p , $x^p - x - a$ is irreducible modulo p .

There is a development of Dedekind's theory of functions modulus p and $F(x)$, where $F(x)$ is irreducible modulo p . Finally, that theory is considered from the point of view of Galois. Just as in the theory of congruences of integers modulo p we treat all multiples of p as if they were zero, so in congruences in the unknown X ,

$$G(X, x) \equiv 0 \pmod{p, F(x)},$$

we operate as if all multiples of $F(x)$ vanish. There is here an indeterminate x which we can make use of to cause the multiples of $F(x)$ to vanish if we agree that this indeterminate x is an imaginary root i of the irreducible congruence $F(x) \equiv 0 \pmod{p}$. From the theorems of the theory of functions modulus p , $F(x)$, we may read off briefer theorems involving i (cf. Galois⁶²).

Harald Schütz⁷⁵ considered a congruence

$$X^n + a_1 X^{n-1} + \dots + a_n \equiv 0 \pmod{M(x)}$$

in which the a 's and the coefficients of M are any complex integers (cf. Cauchy,⁶⁷ for real coefficients). Let a_1, \dots, a_n be the roots of the corresponding algebraic equation. Let $M=0$ have the distinct roots μ_1, \dots, μ_m . Then the congruence has n^m distinct roots. For, let $X - a_p = f_i(x)$ have the factor $x - \mu_i$, for $i=1, \dots, m$. Taking $i > 1$, we have

$$f_i(x) = f_1(x) + a_{p_1} - a_{p_i}.$$

Set $x = \mu_i$. Then the right member must vanish. Using these and $f_1(\mu_1) = 0$, we have m independent linear relations for the coefficients of $f_1(x)$.

C. Jordan⁷⁶ followed Galois in employing from the outset a symbol for an imaginary root of an irreducible congruence, proved the theorems of Galois, and that, if j, j_1, \dots are roots of irreducible congruences of degrees p^a, q^b, \dots where p, q, \dots are distinct primes, their product $jj_1 \dots$ is a root of an irreducible congruence of degree $p^a q^b \dots$.

A. E. Pellet⁷⁷ stated that, if i is a root of an irreducible congruence of degree ν modulo p , a prime, the number of irreducible congruences of degree ν_1 whose coefficients are polynomials in i is

$$\frac{1}{\nu_1} \{ p^{\nu_1} - \Sigma p^{\nu_1/q_1} + \Sigma p^{\nu_1/q_1 q_2} - \dots + (-1)^m p^{\nu_1/q_1 \dots q_m} \}$$

if q_1, \dots, q_m are the distinct primes dividing ν_1 . Of these congruences, $\phi(n)/\nu_1$ belong to the exponent n if n is a proper divisor of $(p^\nu)^{\nu_1} - 1$.

Any irreducible function of degree μ modulo p with integral coefficients is a product of δ irreducible factors of degree μ/δ with coefficients rational in i , where δ is the g. c. d. of μ, ν .

In an irreducible function of degree ν_1 and belonging to the exponent n and having as coefficients rational functions of i , replace x by x^λ , where λ contains only prime factors dividing n ; the resulting function is a product of $2^{k-1}D/n$ irreducible functions of degree $\lambda n \nu_1 / (2^{k-1}D)$ belonging to the exponent λn , where D is the g. c. d. of λn and $p^{\nu_1} - 1$, and 2^{k-1} is the highest power of 2 dividing the numerators of each of the fractions $(p^{\nu_1} + 1)/2$ and $\lambda n / (2D)$ when reduced to their lowest terms.

Let g be a rational function of i , and m the number of distinct values among g, g^p, g^{p^2}, \dots . If neither $g + g^p + \dots + g^{p^{m-1}}$ nor ν/m is divisible by p , then $x^\nu - x - g$ is irreducible; in the contrary case it is a product of linear functions.

Hence if we replace x by $x^p - x$ in an irreducible function of degree μ having as coefficients rational functions of i , we get a new irreducible function provided the coefficient of $x^{\mu-1}$ in the given function is not zero.

⁷⁵Untersuchungen über Functionale Congruenzen, Diss. Göttingen, Frankfurt, 1867.

⁷⁶Traité des substitutions, 1870, 14-18.

⁷⁷Comptes Rendus Paris, 70, 1870, 328-330.

[Proof in Pellet.⁸⁸] In particular, if p is a primitive root of a prime n , we have the irreducible function, modulo p ,

$$\frac{(x^p - x)^n - 1}{x^p - x - 1}.$$

C. Jordan⁷⁸ listed irreducible functions [errata, Dickson,¹⁰² p. 44].

J. A. Serret⁷⁹ determined the product V_n of all functions of degree p^n irreducible modulo p , a prime. In the expansion of $(\xi - 1)^\mu$ replace each power ξ^k by x^{pk} ; denote the resulting polynomial in x by X_μ . Then

$$X_{\nu p^m} \equiv \{(\xi - 1)^{p^m}\}^\nu \equiv (\xi^{p^m} - 1)^\nu, \quad X_{p^m} \equiv x^{p^{p^m}} - x \pmod{p}.$$

Hence $V_n = X_{p^n} / X_{p^{n-1}}$. Moreover,

$$X_{\mu+1} = (\xi - 1)^{\mu+1} = \xi(\xi - 1)^\mu - (\xi - 1)^\mu \equiv X_\mu^p - X_\mu \pmod{p}.$$

Multiply this by the relations obtained by replacing μ by $\mu + 1, \dots, \mu + \nu - 1$. Thus

$$X_{\mu+\nu} \equiv X_\mu (X_\mu^{p-1} - 1)(X_{\mu+1}^{p-1} - 1) \dots (X_{\mu+\nu-1}^{p-1} - 1) \pmod{p}.$$

Take $\mu = p^{n-1}$, $\mu + \nu = p^n$. Hence

$$V_n \equiv \prod_{\lambda=1}^{p^n - p^{n-1}} f_\lambda \pmod{p}, \quad f_\lambda = X_{p^{n-1} + \lambda - 1}^{p-1} - 1.$$

Each f_λ decomposes into $p-1$ factors $X - g$ where $g = 1, \dots, p-1$. The irreducible functions of degree p^n whose product is f_λ are said to belong to the λ th class. When x is replaced by $x^p - x$, X_μ is replaced by $X_{\mu+1}$ since ξ^i is replaced by $\xi^i(\xi - 1)$ and hence $(\xi - 1)^\mu$ by $(\xi - 1)^{\mu+1}$; thus f_λ is replaced by $f_{\lambda+1}$, while the last factor in $V_n = \prod f_\lambda$ is replaced by $X_{p^{n-1}}^{p-1} - 1$, which is the first factor in V_{n+1} . Hence if $F(x)$ is of degree p^n and is irreducible modulo p and belongs to the λ th class, $F(x^p - x)$ is irreducible or the product of p irreducible functions of degree p^n according as $\lambda =$ or $< p^n - p^{n-1}$.

For $n=1$, the irreducible functions of the λ th class have as roots polynomials of degree λ in a root of $i^p - i \equiv 1$, which is irreducible modulo p . Hence if we eliminate i between the latter and $f(i) = x$, where $f(i)$ is the general polynomial of degree λ in i , we obtain the general irreducible function of degree p of the λ th class.

For any n , the determination of the irreducible functions of degree p^n of the first class is made to depend upon a problem of elimination (Algèbre, p. 205) and the relation to these of the functions of the λ th class, $\lambda > 1$, is investigated.

G. Bellavitis^{79a} tabulated the indices of Galois imaginaries of order 2 for each prime modulus $p = 4n + 3 \leq 63$.

Th. Pepin⁸⁰ proved that $x^2 - ny^2 \equiv 1 \pmod{p}$ has $p+1$ sets of solutions

⁷⁸Comptes Rendus Paris, 72, 1871, 283-290.

⁷⁹Jour. de Mathématiques, (2), 18, 1873, 301-4, 437-451. Same as in Cours d'algèbre supérieure, ed. 4, vol. 2, 1879, 190-211.

^{79a}Atti Accad. Lincei, Mem. Sc. Fis. Mat., (3), 1, 1876-7, 778-800.

⁸⁰Atti Accad. Pont. Nuovi Lincei, 31, 1877-8, 43-52.

x, y selected from $0, 1, \dots, p-1$, provided n is a quadratic non-residue of the prime p . Then $x+y\sqrt{n}$ is a root of $\xi^{p+1} \equiv 1 \pmod{p}$, which therefore has $p+1$ complex roots, all a power of one root. There is a table of indices for these roots when $p=29$ and $p=41$. [Lebesgue.⁶³]

A. E. Pellet⁸¹ considered the product Δ of the squares of the differences of the roots of a congruence $f(x) \equiv 0 \pmod{p}$ having no equal roots. Then Δ is a quadratic non-residue of p if $f(x)$ has an odd number of irreducible factors of even degree, a quadratic residue if $f(x)$ has no irreducible factor of even degree or has an even number of them. For, if $\delta_1, \dots, \delta_i$ are the values of Δ for the various irreducible factors of $f(x)$, then $\Delta \equiv a^2 \delta_1 \dots \delta_i \pmod{p}$, where a is an integer. Hence it suffices to consider an irreducible congruence $f(x) \equiv 0 \pmod{p}$. Let ν be its degree and i a root. In

$$y = \prod_{l=1}^{\nu-1} \prod_{k=0}^{l-1} (x^{p^k} - x^{p^l})$$

replace x by the ν roots; we get two distinct values if ν is even, one if ν is odd. In the respective cases, $y^2 \equiv \Delta \pmod{p}$ is irreducible or reducible.

R. Dedekind⁸² noted that, if $P(x)$ is a prime function of degree f modulo p , a prime, a congruence $F(x) \equiv 0 \pmod{p, P}$ is equivalent to the congruence $F(a) \equiv 0 \pmod{\pi}$, where π is a prime ideal factor of p of norm p^f , and a is a root of $P(a) \equiv 0 \pmod{\pi}$.

A. E. Pellet⁸³ denoted by $f(x) = 0$ the equation of degree $\phi(k)$ having as its roots the primitive k th roots of unity, and by $f_1(y) = 0$ the equation derived by setting $y = x + 1/x$. If p is a prime not dividing k , $f(x)$ is congruent modulo p to a product of $\phi(k)/\nu$ irreducible factors whose degree ν is the least integer for which $p^\nu - 1$ is divisible by k . If $f_1(y) \equiv 0 \pmod{p}$ has an integral root a , $f(x)$ is divisible modulo p by $x^2 - 2ax + 1$. Either the latter has two real roots and $f(x)$ and $f_1(y)$ have all their roots real and $p-1$ is divisible by k , or it is irreducible and $f(x)$ is a product of quadratic factors modulo p and the roots of $f_1(y)$ are all real and $p+1$ is divisible by k . If k divides neither $p+1$ nor $p-1$, $f_1(y)$ is a product of factors of equal degree modulo p . [Cf. Sylvester,²⁹ etc., Ch. XVI.]

Let k be a divisor $\neq 2$ of $p+1$. Let λ be an odd number divisible by no prime not a factor of k , and relatively prime to $(p+1)/k$. Then $x^{2\lambda} - 2ax^\lambda + 1$ is irreducible modulo p [Serret,⁷⁴ No. 355]. Also, if b is not divisible by p

$$F = (x+b)^{2\lambda} - 2a(x^2 - b^2)^\lambda + (x-b)^{2\lambda}$$

is irreducible modulo p ; replacing x^2 by y , we obtain a function of degree λ irreducible modulo p . If k is a divisor $\neq 2$ of $p-1$ and if λ is odd, prime to $(p-1)/k$ and divisible by no prime not a factor of k , F decomposes modulo p into two irreducible functions of degree λ .

The function $f(x^2)$ is either irreducible or the product of two irreducible factors of degree ν . In the respective cases, the product Δ of the squares of

⁸¹Comptes Rendus Paris, 86, 1878, 1071-2.

⁸²Abhand. K. Gesell. Wiss. Göttingen, 23, 1878, p. 25. Dirichlet-Dedekind, Zahlentheorie, ed. 4, 1894, 571-2.

⁸³Comptes Rendus Paris, 90, 1880, 1339-41.

the differences of the roots of $f(x^2) \equiv 0$ is a quadratic non-residue or residue of p [Pellet⁸¹]. Let Δ_1 be the like product for $f(x)$. Then $\Delta = (-1)^{\nu} 2^{2\nu} f(0) \Delta_1^2$. Hence $f(ax^2 + b)$ is irreducible if $(-1)^{\nu} f(b)/a^{\nu}$ is a quadratic non-residue and then $f(ax^{2^i} + b)$ is irreducible modulo p for every i and even ν .

O. H. Mitchell⁸⁴ gave analogues of Fermat's and Wilson's theorems modulis p (a prime) and a function of x .

A. E. Pellet⁸⁵ considered the exponent n to which belongs the product P of the roots of a congruence $F(x) \equiv 0$ of degree ν irreducible modulo p . If q is a prime factor of n , $F(x^q)$ is irreducible or the product of q irreducible factors of degree ν modulo p according as q is not or is a divisor of $(p-1)/\nu$. In particular, $F(x^{\lambda})$ is irreducible modulo p if, for ν even, λ contains only prime factors of n not dividing $(p-1)/\nu$; for ν odd, we can use the factor 2 in λ only once if $p = 4m + 1$. Let i be a root of $F(x) \equiv 0$, i_1 a root of an irreducible congruence $F_1(x) \equiv 0 \pmod{p}$ of degree ν_1 prime to ν . Then i_1 is a root of an irreducible congruence $G(x) \equiv 0 \pmod{p}$ of degree $\nu\nu_1$. $F(x)$ belongs to the exponent Nn modulo p , where n is prime to $(p^{\nu}-1) \div \{(p-1)N\}$. Let q_1 be a prime factor of N not dividing $p-1$. Then $G(x^{q_1})$ is irreducible or decomposes into q_1 irreducible factors of degree $\nu\nu_1$ according as q_1 is not or is a divisor of $(p^{\nu}-1)/N$. Thus $G(x^{\lambda})$ is irreducible if λ contains only prime factors of N dividing neither $p-1$ nor $(p^{\nu}-1)/N$.

O. H. Mitchell⁸⁶ defined the prime totient of $f(x)$ to mean the number of polynomials in x , incongruent modulo p , of degree less than the degree of (x) and having no factor in common with f modulo p . Those which contain S , but no prime factor of f not contained in S , are called S -totitives of f .

C. Dina⁸⁷ proved known results on congruences modulis p and $F(x)$.

A. E. Pellet⁸⁸ proved that, if μ distinct values are obtained from a rational function of x with integral coefficients by replacing x successively by the m roots of an irreducible congruence modulo p , then μ is a divisor of m and these μ values are the roots of an irreducible congruence. Thus if A is a rational function of any number of roots of congruences irreducible modulo p , and ν is the number of distinct values among A, A^p, A^{p^2}, \dots , these values satisfy an irreducible congruence modulo p . If A belongs to the exponent n modulo p , then ν is the least positive integer for which $p^{\nu} \equiv 1 \pmod{n}$. He proved a result of Serret's⁷⁴ stated in the following form: If, in an irreducible function $F(x)$ modulo p of degree ν and exponent n , x is replaced by x^{λ} , where λ contains only primes dividing n , then $F(x^{\lambda})$ is a product of irreducible factors of degree νq and exponent $n\lambda$, where q is the least integer for which $p^{q^{\nu}} \equiv 1 \pmod{n\lambda}$. He proved the first theorem of Pellet⁸⁵ and the last one of Pellet.⁷⁷

⁸⁴Johns Hopkins University Circulars, 1, 1880-1, 132.

⁸⁵Comptes Rendus Paris, 93, 1881, 1065-6. Cf. Pellet.⁸⁶

⁸⁶Amer. Jour. Math., 4, 1881, 25-38.

⁸⁷Giornale di Mat., 21, 1883, 234-263. For comments on 263-9, see the chapter on quadratic reciprocity law.

⁸⁸Bull. Soc. Math. France, 17, 1888-9, 156-167.

E. H. Moore⁸⁹ stated that every finite field (Körper) is, apart from notations, a Galois field composed of the p^n polynomials in a root of an irreducible congruence of degree n modulo p , a prime.

E. H. Moore⁹⁰ proved the last theorem and others on finite fields.

K. Zsigmondy³⁶ noted that the number of congruences of degree n modulo p , having no irreducible factor of degree i , is

$$p^n - \binom{I}{1} p^{n-i} + \binom{I}{2} p^{n-2i} - \dots,$$

where I is the number of functions of degree i irreducible modulo p .

G. Cordone⁹¹ noted that if a function is prime to each of its derivatives with respect to each prime modulus p_1, \dots, p_n and is irreducible modulo $M = p_1^{e_1} \dots p_n^{e_n}$, it is irreducible with respect to at least one of p_1, \dots, p_n . If $F(x)$ is not identically $\equiv 0$ modulo p_1 , nor modulo p_2 , etc., and if it divides a product modulo M and is prime to one factor according to each modulus p_1, \dots, p_n , then $F(x)$ divides the other factor modulo M .

Let $F(x)$ be a function of degree r irreducible with respect to each prime p_1, \dots, p_n , while $f(x)$ is not divisible by $F(x)$ with respect to any one of the p 's, then (pp. 281-8)

$$\{f(x)\}^{\phi_r(M)} \equiv 1 \pmod{M, F(x)}, \quad \phi_r(M) = M^r \left(1 - \frac{1}{p_1^r}\right) \dots \left(1 - \frac{1}{p_n^r}\right),$$

$\phi_r(M)$ being the number of functions $c_1 x^{r-1} + \dots + c_r$, in which the c 's take such values $0, 1, \dots, M-1$ whose g. c. d. is prime to M . Let A be the product of these reduced functions modulus $M, F(x)$. Then (pp. 316-8), $A \equiv -1 \pmod{M, F}$ if $M = p^k, 2p^k$ or 4 , where p is an odd prime, while $A \equiv +1$ in all other cases.

Borel and Drach⁹² gave an exposition of the theory of Galois imaginaries from the standpoint of Galois himself.

H. Weber⁹³ considered the finite field (Congruenz Körper) formed of the p^n classes of residues modulo p of the polynomials, with integral coefficients, in a root of an irreducible equation of degree n . He proved the generalization of Fermat's theorem, the existence of primitive roots, and the fact that every element is a square or a sum of the squares of two elements.

Ivar Damm⁹⁴ gave known facts about the roots of congruences modulus $p, f(x)$, where $f(x)$ is irreducible modulo p , without exhibiting the second modulus and without making it clear that it is not a question of ordinary congruences modulo p . Let e be a fixed primitive root of the prime p . Then the roots of every irreducible quadratic congruence are of the form $a \pm b\omega$, where $\omega^2 = e$. Let $k^{p+1} = e, k_1 = k^p$.

⁸⁹Bull. New York Math. Soc., 3, 1893-4, 73-8.

⁹⁰Math. Papers Chicago Congress of 1893, 1896, 208-226; University of Chicago Decennial Publications, (1), 9, 1904, 7-19.

⁹¹El Progreso Matemático, 4, 1894, 265-9.

⁹²Introd. théorie des nombres, 1895, 42-50, 58-62, 343-350.

⁹³Lehrbuch der Algebra, II, 1896, 242-50, 259-261; ed. 2, 1899, 302-10, 320-2.

⁹⁴Bidrag till Lära om Kongruenser med Primtalsmodul, Diss., Upsala, 1896, 86 pp.

Analogous to the definition of trigonometric functions in terms of exponentials, he defined quasi cosines and sines by

$$Cqx = \frac{1}{2}(k^x + k_1^x), \quad Sqx = \frac{1}{2\omega}(k^x - k_1^x),$$

and Tqx as their quotient. Their relations are discussed. He defined pseudo cosines and sines by

$$Cpx = Cq[(p-1)x] = e^{-x}Cq2x, \quad Spx = -e^{-x}Sq2x.$$

For each prime $p < 100$, he gave (pp. 65-86) the (integral) values of

$$e^x, \text{ and } x, Cqx, Sqx, Tqx, Cpx, Spx$$

for $x = 1, 2, \dots, p+1$.

L. E. Dickson⁹⁵ extended the results of Serret⁷⁴ to the more general case in which the coefficients of the functions are polynomials in a given Galois imaginary (i. e., are in a Galois field of order p^n). For the corresponding generalization of the results of Serret⁷⁹ on irreducible congruences modulo p of degree a power of p , additional developments were necessary. To obtain the irreducible functions of degree p in the $GF[p^n]$ which are of the first class, we need the complete factorization, in the field,

$$h(z^{p^n} - z - \nu) = \Pi(h^p z^p - hz - \beta)$$

where $h\nu$ is an integer and β ranges over the roots of

$$B = \beta^{p^n-1} + \beta^{p^n-2} + \dots + \beta^p + \beta = h\nu,$$

all of whose roots are in the field. For the case $\nu = 0$ this factorization is due to Mathieu.⁷³ Thus $h^p z^p - hz - \beta$ is irreducible in the field if and only if $B \neq 0$. In particular, if β is an integer not divisible by p , $z^p - z - \beta$ is irreducible in the $GF[p^n]$ if and only if n is not divisible by p .

R. Le Vavas seur⁹⁶ employed Galois imaginaries to express in brief notation the groups of isomorphisms of certain types of groups, for example, that of the abelian group G generated by n independent operators a_1, \dots, a_n , each of period a prime p . If i is a root of an irreducible congruence of degree n modulo p , and if $j = a_1 + ia_2 + \dots + i^{n-1}a_n$, he defined a^j to be $a_1^{a_1} \dots a_n^{a_n}$. Then the operators of G are represented by the real and imaginary powers of a .

A. Guldberg⁹⁷ considered linear differential forms

$$Ay = a_k \frac{d^k y}{dx^k} + \dots + a_1 \frac{dy}{dx} + a_0 y,$$

with integral coefficients. The product of two such forms is defined by Boole's symbolic method to be

$$Ay \cdot By = (a_k \frac{d^k}{dx^k} + \dots + a_0)(b_l \frac{d^l}{dx^l} + \dots + b_1 \frac{d}{dx} + b_0)y.$$

⁹⁵Bull. Amer. Math. Soc., 3, 1896-7, 381-9.

⁹⁶Mém. Ac. Sc. Toulouse, (9), 9, 1897, 247-256.

⁹⁷Comptes Rendus Paris, 125, 1897, 489.

If the product is $\equiv Cy \pmod{p}$, Ay and By are called divisors modulo p of Cy . Let Δy be of order n and irreducible modulo p . Then Ay is congruent modulus p , Δy to one and but one of the p^n forms

$$(4) \quad \sum_{i=0}^{n-1} c_i \frac{d^i y}{dx_i} \quad (c_i = 0, 1, \dots, p-1).$$

If u is any one of these forms (4) and if $e = p^n - 1$, Guldberg stated the analogue of Fermat's theorem

$$\frac{d^e u}{dx^e} \equiv u \pmod{p, \Delta y},$$

but incorrectly gave the right member to be unity [cf. Epstein,¹⁰⁶ Dickson¹⁰⁷].

L. Stickelberger⁹⁸ considered $F(x) = x^n + a_1 x^{n-1} + \dots$ with integral coefficients, such that the product D of the squares of the differences of the roots is not zero. Let p be any prime not dividing D . Let ν be the number of factors of $F(x)$ which are irreducible modulo p . He proved by the use of prime ideals that

$$\left(\frac{D}{p}\right) = (-1)^{n-\nu},$$

where the symbol in the left member is that of Legendre [see quadratic residues].

L. E. Dickson⁹⁹ proved the existence of the Galois field $GF[p^r]$ of order p^n by induction from $r=n$ to $r=qn$, by showing that

$$(x^{p^{nq}} - x) / (x^{p^n} - x)$$

is a product of factors of degree q belonging to and irreducible in the $GF[p^n]$. Any such factor defines the $GF[p^{nq}]$.

L. Kronecker¹⁰⁰ treated congruences modulus p , $P(x)$ from the standpoint of modular systems.

F. S. Carey¹⁰¹ gave for each prime $p < 100$ a table of the residues of the first $p+1$ powers of a primitive root $a+bj$ of $z^{p^2-1} \equiv 1 \pmod{p}$ where $j^2 \equiv \nu \pmod{p}$, ν being an integral quadratic non-residue of p . The higher powers are readily derived. While only the single modulus p is exhibited, it is really a question of a double modulus p and $x^2 - \nu$. Methods of "solving" $z^{p^n-1} \equiv 1$ are discussed. In particular, for $n=3$, there is given a primitive root for each prime $p < 100$.

L. E. Dickson¹⁰² gave a systematic introductory exposition of the theory, with generalizations and extensions.

M. Bauer¹⁰³ proved that, if $f(x) = 0$ is an irreducible equation with integral coefficients and leading coefficient unity, w a root, D its discriminant, $d = D/k^2$ that of the domain defined by w , p a prime not dividing k , $x > 1$,

⁹⁸Verhand. I. Internat. Math. Kongress, 1897, 186.

⁹⁹Bull. Amer. Math. Soc., 6, 1900, 203-4.

¹⁰⁰Vorlesungen über Zahlentheorie, I, 1901, 212-225 (expanded by Hensel, p. 506).

¹⁰¹Proc. London Math. Soc., 33, 1900-1, 294-310.

¹⁰²Linear groups with an exposition of the Galois field theory, Leipzig, 1901, pp. 1-71.

¹⁰³Math. Naturw. Berichte aus Ungarn, 20, 1902, 39-42; Math. és Phys. Lapok, 10, 1902, 28-33.

then $f(x)$ is congruent modulo p^a to a product of $F_1(x), \dots, F_s(x)$, each irreducible modulo p^a , such that $F_i(x) \equiv f_i(x)^{e_i} \pmod{p}$, where $f(x) \equiv \prod f_i(x)^{e_i} \pmod{p}$, and $f_i(x)$ is irreducible modulo p . There is an example of an irreducible cyclotomic function reducible with respect to every prime power modulus.

P. Bachmann¹⁰⁴ gave an exposition of the general theory.

G. Arnoux¹⁰⁵ exhibited in the form of tables the work of finding a primitive root of the $GF[7^3]$ and of the $GF[5^4]$, and tabulated the reducible and irreducible congruences of degrees 1, 2, 3, modulo 5.

S. Epstein¹⁰⁶ proved the result of Guldberg,⁹⁷ and developed the theory of residues of linear differential forms parallel to the theory of finite fields, as presented by Dickson.¹⁰²

L. E. Dickson¹⁰⁷ noted that the last mentioned subjects are identical abstractly. Let the irreducible form Δy be

$$\delta_n \frac{d^n y}{dx^n} + \dots + \delta_1 \frac{dy}{dx} + \delta_0 y.$$

To the element (4) we make correspond the element $\Sigma c_i z^i$ of the Galois field of order p^n , where z is a root of the irreducible congruence

$$\delta_n z^n + \dots + \delta_1 z + \delta_0 \equiv 0 \pmod{p}.$$

Since product relations are preserved by this correspondence, the p^n residues (4) define a field abstractly identical with our Galois field.

Dickson^{107a} proved that $x^m \equiv x \pmod{m=p^n}$ has p and only p roots if p is a prime and hence does not define the Galois field of order m as occasionally stated.

A. Guldberg^{107b} employed the notation of finite differences and wrote

$$Fy_x = \sum_{i=0}^n a_i \theta^i y_x, \quad Gy_x = \sum_{i=0}^m b_i \theta^i y_x, \quad Fy_x \cdot Gy_x = \sum_{i=0}^n a_i \theta^i \cdot \sum_{i=0}^m b_i \theta^i y_x,$$

where $\theta y_x = y_{x+1}$, $\theta^2 y_x = y_{x+2}$, ..., symbolically. To these linear forms with integral coefficients taken modulo p , a prime, we may apply Euclid's g. c. d. process and prove that factorization is unique. Next, let b_m be not divisible by p , so that Gy_x is of order m . With respect to the two moduli p , Gy_x , a complete set of p^m residues of linear forms is $a_{m-1} y_{x+m-1} + \dots + a_0 y_x$ ($a_i = 0, 1, \dots, p-1$). Amongst these occur $\phi(Gy_x) = p^m(1-1/p^{m_1}) \dots (1-1/p^{m_q})$ forms Fy_x prime to Gy_x if m_1, \dots, m_q are the orders of the irreducible factors of Gy_x modulo p , and

$$Fy_x^{\phi(Gy_x)} \equiv y_x \pmod{p, Gy_x}$$

In particular, if Gy_x is irreducible and of order m ,

$$Fy_x^{p^m-1} \equiv y_x \pmod{p, Gy_x}.$$

¹⁰⁴Niedere Zahlentheorie, 1, 1902, 363-399.

¹⁰⁵Assoc. franç. av. sc., 31, 1902, II, 202-227.

¹⁰⁶Bull. Amer. Math. Soc., 10, 1903-4, 23-30.

¹⁰⁷Ibid., pp. 30-1.

^{107a}Amer. Math. Monthly, 11, 1904, 39-40.

^{107b}Annali di Mat., (3), 10, 1904, 201-9.

W. H. Bussey¹⁰⁸ gave for each Galois field of order <1000 companion tables showing the residues of the successive powers of a primitive root, and the powers corresponding to the residues arranged in a natural order. These tables serve the same purposes in computations with Galois fields that tables of indices serve in computations with integers modulo p^n , where p is a prime.

G. Voronoï¹⁰⁹ proved the theorem of Stickelberger.⁹⁸ Thus, for $n=3$, $(D/p)=-1$ only when $\nu=2$. Hence a cubic congruence has a single root if $(D/p)=-1$, and three real roots or none if $(D/p)=+1$.

P. Bachmann¹¹⁰ developed the general theory from the standpoint of Kronecker's modular systems and considered its relation to ideals (p. 241).

M. Bauer¹¹¹ employed a polynomial $f(z)$ of degree n irreducible modulo p , and another one $M(z)$ of degree less than that of $f'(z)$ and not divisible by $f(z)$ modulo p . Then if $(t, a)=1$, the equation

$$f'(z) + p^a M(z) = 0$$

is irreducible. The case $a=1$ is due to Schönemann⁶⁵ (p. 101).

G. Arnoux,¹¹² starting with any prime m and integer n , introduced a symbol i such that $i^s \equiv 1 \pmod{m}$ and such that i, i^2, \dots, i^s are distinct, where $s=m^n-1$, without attempting a logical foundation. If $f(x)$ is irreducible modulo m and of degree n , there is only a finite number of distinct residues of powers of x modulus $f(x), m$; let x^k and x^{k+p} have the same residue. Thus x^p-1 is divisible by $f(x)$ modulo m . It is stated (p. 95) without proof that p divides s . "Call a a root of $f(x) \equiv 0$. To make a coincide with the primitive root i of $x^s=1$, we must take $p=s$, whence every such primitive root is a root of an irreducible congruence of degree n modulo m ." Following this inadequate basis is an exposition (pp. 117-136) of known properties of Galois imaginaries.

L. I. Neikirk¹¹³ represented geometrically the elements of the Galois field of order p^n defined by an irreducible congruence

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{p}.$$

Let j be a root of the equation $f(x)=0$ and represent

$$c_1 j^{n-1} + \dots + c_{n-1} j + c_n \quad (c's \text{ integers})$$

by a point in the complex plane. The p^n points for which the c 's are chosen from $0, 1, \dots, p-1$ represent the elements of the Galois field.

G. A. Miller¹¹⁴ listed all possible modular systems $p, \phi(x)$, where p is a prime and the coefficient of the highest power of x is unity, in regard to which a complete set of prime residues forms a group of order ≤ 12 . If $\phi(x)$ is the product of k distinct irreducible functions ϕ_1, \dots, ϕ_k modulo p ,

¹⁰⁸Bull. Amer. Math. Soc., 12, 1905, 21-38; 16, 1909-10, 188-206.

¹⁰⁹Verhand. III. Internat. Math. Kongress, 1905, 186-9.

¹¹⁰Allgemeine Arith. d. Zahlenkörper, 1905, 81-111.

¹¹¹Jour. für Math., 128, 1905, 87-9.

¹¹²Arithmétique Graphique, Fonctions Arith., 1906, 91-5.

¹¹³Bull. Amer. Math. Soc., 14, 1907-8, 323-5.

¹¹⁴Archiv Math. Phys., (3), 15, 1909-10, 115-121.

the residues prime to p , $\phi(x)$ constitute the direct product of the groups with respect to the various p , $\phi_i(x)$. Not every abelian group can be represented as a congruence group composed of a complete set of prime residues with respect to F_1, \dots, F_λ , where the F 's are functions of a single variable.

Mildred Sanderson¹¹⁵ employed two moduli m and $P(y)$, the first being any integer and the second any polynomial in y with integral coefficients. Such a polynomial $f(y)$ is said to have an inverse $f_1(y)$ if $ff_1 \equiv 1 \pmod{m, P}$. If $P(y)$ is of degree r and is irreducible with respect to each prime factor of m , a function $f(y)$, whose degree is $< r$, has an inverse modulus $m, P(y)$, if and only if the g. c. d. of the coefficients of $f(y)$ is prime to m . For such an f , $f^n \equiv 1 \pmod{m, P}$, where n is Jordan's function $J_r(m)$ [Jordan,²⁰⁰ Ch. V]. In case m is a prime, this result becomes Galois'⁶² generalization of Fermat's theorem. The product of the n distinct residues having inverses modulus $m, P(y)$, is congruent to -1 when m is a power of an odd prime or the double of such a power or when $r=1, m=4$; but congruent to $+1$ in all other cases—a two-fold generalization of Wilson's theorem. There exists a polynomial $P(y)$ of degree r which is irreducible with respect to each prime factor of m . Then if $A(y), B(y)$ are of degrees $< r$ and their coefficients are not all divisible by a factor of m , there exist polynomials $\alpha(y), \beta(y)$, such that $\alpha A + \beta B \equiv 1 \pmod{m, P}$.

Several writers¹¹⁶ discussed the irreducible quadratic factors modulo p of $(x^a - 1)/(x^k - 1)$, where $k=1$ or 2 , p is a prime, a a divisor of $p+1$.

G. Tarry¹¹⁷ noted that, if $j^2 \equiv q \pmod{m}$, where q is a quadratic non-residue of the prime m , the Galois imaginary $a+bj$ is a primitive root if its norm $(a+bj)(a-bj)$ is a primitive root of m and if the ratio $a:b$ and the analogous ratios of the coordinates of the first m powers of $a+bj$ are incongruent.

L. E. Dickson¹¹⁸ proved that two polynomials in two variables with integral coefficients have a unique g. c. d. modulo p , a prime. Thus the unique factorization theorem holds.

G. Tarry¹¹⁹ stated that $A\rho$ is a primitive root of the $GF[p^2]$ if the norm of $A=a+bj$ is a primitive root of p and if the imaginary ρ belongs to the exponent $p+1$. The $\phi(p+1)$ numbers ρ are found by the usual process to obtain the primitive roots of a prime.

U. Scarpis¹²⁰ proved that an equation of degree ν irreducible in the Galois field of order p^n has in the field of order p^{mn} either ν roots or no root according as ν is or is not a divisor of m [Dickson¹⁰², p. 19, lines 7-9].

CUBIC CONGRUENCES.

A. Cauchy¹³⁰ solved $y^3 + By + C \equiv 0 \pmod{p}$ when it has three distinct

¹¹⁵Annals of Math., (2), 13, 1911, 36-9.

¹¹⁶L'intermédiaire des math., 18, 1911, 195, 246; 19, 1912, 61-69, 95-6; 21, 1914, 153-161; 22, 1915, 77-8. Sphinx-Oedipe, 7, 1912, 2-3.

¹¹⁷Assoc. franç. av. sc., 40, 1911, 12-24.

¹¹⁸Bull. Amer. Math. Soc., (2), 17, 1911, 293-4.

¹¹⁹Sphinx-Oedipe, 7, 1912, 43-4, 49-50.

¹²⁰Annali di Mat., (3), 23, 1914, 45.

¹³⁰Exercices de Math., 4, 1829, 279-292; Oeuvres, (2), 9, 326-333.

integral roots y_1, y_2, y_3 , and p is a prime $\equiv 1 \pmod{3}$, and $B \not\equiv 0 \pmod{p}$. Set

$$3v_1 = y_1 + ry_2 + r^2y_3, \quad 3v_2 = y_1 + r^2y_2 + ry_3, \quad r^2 + r + 1 \equiv 0 \pmod{p}.$$

The roots of $u^2 + Cu - B^3/27 \equiv 0 \pmod{p}$ are $u_1 = v_1^3, u_2 = v_2^3$. After finding v_1 from $v_1^3 \equiv u_1 \pmod{p}$, we get $v_2 \equiv -B/(3v_1)$, and determine the y 's from $\Sigma y_i \equiv 0$ and the expressions for $3v_1, 3v_2$. Thus

$$y_1 \equiv v_1 + v_2, \quad y_2 \equiv r^2v_1 + rv_2, \quad y_3 \equiv rv_1 + r^2v_2 \pmod{p}.$$

Since by hypothesis the cubic congruence has three distinct integral roots, the quadratic has two distinct integral roots, whence

$$\begin{aligned} u_i^{\frac{p-1}{3}} &\equiv 1, & D^{\frac{p-1}{2}} &\equiv 1 \pmod{p}, & D &= \frac{C^2}{4} + \frac{B^3}{27}, \\ \left(-\frac{C}{2} - D^{\frac{1}{2}}\right)^{\frac{p-1}{3}} + \left(-\frac{C}{2} + D^{\frac{1}{2}}\right)^{\frac{p-1}{3}} &\equiv 2, & D^{\frac{p-1}{2}} &\equiv 1 \pmod{p}. \end{aligned}$$

Conversely, if the last two conditions are satisfied, the cubic congruence has three distinct real roots provided $p \equiv 1 \pmod{3}$, $B \not\equiv 0 \pmod{p}$.

G. Oltramare¹³¹ found the conditions that one or all of the roots of $x^3 + 3px + 2q \equiv 0 \pmod{\mu}$ given by Cardan's formula become integral modulo μ , a prime. Set

$$D = q^2 + p^3, \quad \sigma = -q + \sqrt{D}, \quad \tau = -q - \sqrt{D},$$

First, let μ be a prime $6n-1$. If D is a quadratic residue of μ , there is a single rational root $-2q/(p + \sigma^{2n} + \tau^{2n})$. If D is a quadratic non-residue of μ , there are three rational roots or no root according as the rational part M of the development of σ^{2n-1} by the binomial theorem satisfies or does not satisfy $Mp^2 + q \equiv 0 \pmod{\mu}$; if also $\mu = 18m+11$ and there are three rational roots, they are

$$2M\sqrt[3]{p^2}, \quad -\sqrt[3]{p^2}(M \pm N\sqrt{-3D}),$$

if $\sigma^{2m+1} = M + N\sqrt{D}$; with a like result when $\mu = 18m+5$.

Next, let $\mu = 6n+1$. If D is a quadratic non-residue of μ , there is one rational root or none according as the rational part M of the development of σ^{2n} is or is not such that

$$(2M-1)^2(M+1) \equiv -2q^2/p^3 \pmod{\mu},$$

and if a rational root exists it is $2q/\{p(2M-1)\}$. If D is a quadratic residue of μ , there are three rational roots or none according as $\sigma^{2n} \equiv 1 \pmod{\mu}$ or not. When there are three, they are given explicitly if $\mu = 18m+7$ or $18m+13$, while if $\mu = 18m+1$ there are sub-cases treated only partially.

G. T. Woronoi¹³² (or Voronoï) employed Galois imaginaries $a+bi$, where $i^2 - N \equiv 0 \pmod{p}$ is irreducible, p being an odd prime, to treat the solution of

$$x^3 - rx - s \equiv 0 \pmod{p}.$$

¹³¹Jour. für Math., 45, 1853, 314-339.

¹³²Integral algebraic numbers depending on a root of a cubic equation (in Russian), St. Petersburg, 1894, Ch. I. Cf. Fortschritte Math., 25, 1893-4, 302-3. Cf. Voronoï.¹⁰⁹

If $4r^3 - 27s^2$ is a quadratic non-residue of p , the congruence has one and only one root; but if it is a residue, there are three roots or no root.

G. Cordone¹³³ gave simpler proofs of Oltramare's¹³¹ theorem II on the case $\mu = 6n - 1$, gave theorems to replace VII and VIII, and proved that the condition in IX is sufficient as well as necessary.

Ivar Damm⁹⁴ found when Cardan's formula gives three real roots, one or no real root of a cubic congruence, and expressed the roots by use of his quasi sine and cosine functions. For the prime modulus $p = 3n + 1$, $f = x^3 + ax + b$ is irreducible if

$$c = \sqrt{\frac{b^2}{4} + \frac{a^3}{27}} \text{ is real, } \left(-\frac{b}{2} + c\right)^{\frac{p-1}{6}} \equiv \pm 1.$$

If $p = 3n - 1$, it is irreducible if c and $(-b/2 + c)^n$ are both imaginary. There are given (p. 52) explicit expressions for b such that f is irreducible.

J. Iwanow¹³⁴ gave another proof of the theorem of Woronoj.¹³²

Woronoj¹³⁵ gave another proof of the same theorem and stated that the congruence has the same number of roots for all primes representable by a binary quadratic form whose determinant equals $-4r^3 + 27s^2$.

G. Arnoux¹³⁶ gave double-entry tables of the roots of the congruences $x^3 + bx^2 + a \equiv 0 \pmod{m}$, and solved numerical cubic congruences by interpreting Cardan's formulas.

G. Arnoux¹³⁷ treated $x^3 + bx + a \equiv 0 \pmod{m}$ by use of Cardan's formula. For $m = 11$, he gave a table of the real roots for $a \leq 10$, $b \leq 10$, and the residues of

$$R = \frac{a^2}{4} + \frac{b^3}{27}.$$

When R is a quadratic residue, the cube roots of $-a/2 \pm \sqrt{R}$ are found by use of a table for the Galois field of order 11^2 defined by $i^2 \equiv 2 \pmod{11}$, and the cubic is seen to have a real and two imaginary roots involving i . If R is a quadratic non-residue, there are three real roots or none. Like results are said to hold when $m - 1$ is not divisible by 3. If $m \equiv 1 \pmod{3}$, there is a single real root if R is a quadratic non-residue; three real or three imaginary roots of the third order if R is a residue.

L. E. Dickson¹³⁸ proved that, if p is a prime > 3 , $x^3 + \beta x + b \equiv 0 \pmod{p}$ has no integral root if and only if $-4\beta^3 - 27b^2$ is a quadratic residue of p , say $\equiv 81\mu^2$, and if $\frac{1}{2}(-b + \mu\sqrt{-3})$ is not congruent to the cube of any $y + z\sqrt{-3}$, where y and z are integers. The reducible and irreducible cubic congruences are given explicitly. Necessary and sufficient conditions for the irreducibility of a quartic congruence are proved.

¹³³Rendiconti Circolo Mat. di Palermo, 9, 1895, 221-36.

¹³⁴Bull. Ac. Sc. St. Petersburg, 5, 1896, 137-142 (in Russian).

¹³⁵Natural Sc. (Russian), 10, 1898, 329; cf. Fortschritte Math., 29, 1898, 156.

¹³⁶Assoc. franç. av. sc., 30, 1901, II, 31-50, 51-73; corrections, 31, 1902, II, 202.

¹³⁷Assoc. franç. av. sc., 33, 1904, 199-230 [182-199], and Arnoux¹¹², 166-202.

¹³⁸Bull. Amer. Math. Soc., 13, 1906, 1-8.

D. Mirimanoff¹³⁹ noted that the results by Arnoux^{112, 137} may be combined by use of the discriminant $D = -4b^3 - 27a^2 = -3 \cdot 6^2 R$ in place of R , since -3 is a quadratic residue of a prime $p = 3k + 1$, non-residue of $p = 3k - 1$, and we obtain the result as stated by Voronoï.¹³²

To find which of the values 1 or 3 is taken by ν when D is a quadratic residue, apply the theorem that if $f(x) \equiv 0 \pmod{p}$ is an irreducible congruence of degree n and if x_0 is one of its imaginary roots (say one of the roots of the equation $f(x) = 0$), the roots are

$$x_0, \quad x_1 = x_0^p, \dots, \quad x_{n-1} = x_0^{p^{n-1}}.$$

Hence a function unaltered by the cyclic substitution $(x_0 x_1 \dots x_{n-1})$ has an integral value modulo p . Take $n = 3$, $D \equiv d^2$, a a root $\not\equiv 1$ of $z^3 \equiv 1 \pmod{p}$, and let

$$M = (x_0 + ax_1 + a^2 x_2)^3.$$

If $p \equiv 1 \pmod{3}$, a is an integer, and M is an integer if $\nu = 1$, while M is the cube of an integer if $\nu = 3$. Thus we have Arnoux's criterion:¹¹² $\nu = 3$ if M or $\frac{3}{2}(-9a + \sqrt{-3d})$ is a cubic residue modulo p . If $p \equiv -1 \pmod{3}$ $\nu = 3$ if and only if $M^k \equiv 1 \pmod{p}$, where $k = (p^2 - 1)/3$.

For quartic congruences, we can use $(x_0 - x_1 + x_2 - x_3)^2$.

R. D. von Sterneck¹⁴⁰ noted that if p is a prime > 3 not dividing A , and if $k = 3AC - B^2 \not\equiv 0 \pmod{p}$, then the number of incongruent values taken by $Ax^3 + Bx^2 + Cx + D$ is $\frac{1}{3}\{2p + (-3/p)\}$; but, if $k \equiv 0$, the number is p if $p = 3n - 1$, $(p + 2)/3$ if $p = 3n + 1$. Generalization by Kantor.¹⁸¹

C. Cailler¹⁴¹ treated $x^3 + px + q \equiv 0 \pmod{l}$, where l is a prime > 3 . By the algebraic method leading to Cardan's formula, we write the congruence in the form

$$(1) \quad x^3 - 3abx + ab(a + b) \equiv 0 \pmod{l},$$

where a, b are the roots of $z^2 + 3qz/p - p/3 \equiv 0 \pmod{l}$, whence

$$z \equiv (x_0 + ax_1 + a^2 x_2)^3 / (9p), \quad a^2 + a + 1 \equiv 0 \pmod{l}.$$

Let $\Delta = 4p^3 + 27q^2$. If 3Δ is a quadratic residue of l , a and b are distinct and real. If 3Δ is a non-residue, a and b are Galois imaginaries $r \pm s\sqrt{N}$, where N is any non-residue. For a root x of (1),

$$y^3 \equiv \frac{a}{b} \pmod{l}, \quad y = \frac{x - a}{x - b}.$$

Use is made of a recurring series S with the scale of relation $[a + b, -ab]$ to get y_0, y_1, \dots . Write $Q = (3\Delta/l)$. If $l = 3m - 1$, $Q = 1$, then

$$y \equiv (b/a)^{m-1}, \quad x \equiv \frac{a^m - b^m}{a^{m-1} - b^{m-1}} = \frac{y_m}{y_{m-1}}.$$

If $l = 3m + 1$, $Q = 1$, the congruence is possible only when the real number a/b is a cubic residue, i. e., if $y_m \equiv 0$ in S ; let a/b belong to the exponent $3\mu \equiv 1$ modulo l , whence

¹³⁹L'enseignement math., 9, 1907, 381-4.

¹⁴⁰Sitzungsber. Ak. Wiss. Wien (Math.), 116, 1907, IIa, 895-904.

¹⁴¹L'enseignement math., 10, 1908, 474-487.

$$y \equiv \left(\frac{a}{b}\right)^{\pm \mu}, \quad x \equiv \frac{y_{2\mu}}{y_{2\mu-1}} \text{ or } \frac{y_{\mu+1}}{y_{\mu}},$$

according as the upper or lower sign holds. If $l=3m+1$, $Q=-1$, then

$$y_{3m+2} \equiv 0, \quad \left(\frac{a}{b}\right)^{3m+3} \equiv \frac{a}{b}, \quad \text{real } x \equiv \frac{y_{2m+2}}{y_{2m+1}}.$$

If $l=3m-1$, $Q=-1$, there are three real roots if and only if a/b is a cubic residue of l , viz., $y_m \equiv 0$; when real, the roots may be found as in the second case.

Cailler¹⁴² noted that a cubic equation $X=0$ has its roots expressible rationally in one root and $\sqrt{\Delta}$, where Δ is the discriminant (Serret's *Algèbre*, ed. 5, vol. 2, 466-8). Hence, if p is a prime, $X \equiv 0 \pmod{p}$ has three real roots if one, when and only when Δ is a quadratic residue of p . If $p=9m \pm 1$, his¹⁴¹ test shows that $x^3-3x+1 \equiv 0 \pmod{p}$ has three real roots, but no real root for other prime moduli $\neq 3$. The function $F(x)=x^3+x^2-2x-1$ for the three periods of the seventh roots of unity is divisible by the primes $7m \pm 1$ (then 3 real roots, Gauss⁶⁰, p. 624) and 7, but by no other primes.

E. B. Escott¹⁴³ noted that the equation $F(x)=0$ last mentioned has the roots $\alpha, \beta=\alpha^2-2, \gamma=\beta^2-2$, so that $F(x) \equiv 0 \pmod{p}$ has three real roots if one real root. To find the most general irreducible cubic equation with roots α, β, γ such that

$$\beta=f(\alpha), \quad \gamma=f(\beta), \quad \alpha=f(\gamma),$$

we may assume that $f(x)$ is of degree 2. For $f(\alpha)=\alpha^2-n$, we get

$$(2) \quad x^3+ax^2-(a^2-2a+3)x-(a^3-2a^2+3a-1)=0,$$

with $\beta=\alpha^2-c, \gamma=\beta^2-c, \alpha=\gamma^2-c, c=\alpha^2-a+2$. The corresponding congruence has three real roots if one. To treat $f(\alpha)=\alpha^2+ka+l$, add $k/2$ to each root. For the new roots, $\beta'=\alpha'^2-n$, as in the former case. To treat $f(\alpha)=t\alpha^2+ga+h$, the products of the roots by t satisfy the preceding relation.

L. E. Dickson¹⁴⁴ determined the values of a for which the congruence corresponding to (2) has three integral roots. Replace x by $z-a$; we get

$$z^3-2az^2+(2a-3)z+1 \equiv 0 \pmod{p}.$$

If one root is z , the others are $1-1/z$ and $1/(1-z)$. Evidently a is rational in z . If -3 is a quadratic non-residue of p , there are exactly $(p-2)/3$ values of a for which the congruence has three distinct integral roots. If -3 is a residue, the number is $(p+2)/3$. A second method, yielding an explicit congruence for these values of a , is a direct application of his¹³⁸ general criteria for the nature of the roots of a cubic congruence.

T. Hayashi¹⁴⁵ treated cyclotomic cubic equations with three real roots by use of Escott's¹⁴³ results.

¹⁴²*L'intermédiaire des math.*, 16, 1909, 185-7.

¹⁴³*Annals of Math.*, (2), 11, 1909-10, 86-92.

¹⁴⁴*Ibid.*, (2), 12, 1910-11, 149-152.

¹⁴⁵*Ibid.*, 189-192.

MISCELLANEOUS RESULTS ON CONGRUENCES.

Linear congruences will be treated in Vol. 2 under linear diophantine equations, quadratic congruences in two or more variables, under sums of four squares; $ax^n + by^n + cz^n \equiv 0$, under Fermat's last theorem.

Fermat¹⁴⁸ stated that not every prime p divides one of the numbers $a+1, a^2+1, a^3+1, \dots$. For, if k is the least value for which $a^k - 1$ is divisible by p and if k is odd, no term $a^h + 1$ is divisible by p . But if k is even, $a^{k/2} + 1$ is divisible by p .

Fermat¹⁴⁹ stated that no prime $12n \pm 1$ divides $3^x + 1$, every prime $12n \pm 5$ divides certain $3^x + 1$, no prime $10n \pm 1$ divides $5^x + 1$, every prime $10n \pm 3$ divides certain $5^x + 1$, and intimated that he possessed a rule relating to all primes. See Lipschitz.¹⁶⁶

A. M. Legendre¹⁵⁰ obtained from a given congruence $x^n \equiv ax^{n-1} + \dots \pmod{p}$, p an odd prime, one having the same roots, but with no double roots. Express $x^{(p-1)/2}$ in terms of the powers of x with exponents $< n$, and equate the result to $+1$ and to -1 in turn. The g. c. d. of each and the given congruence is the required congruence. An exception arises if the proposed congruence is satisfied by $0, 1, \dots, p-1$.

Hoëné de Wronski¹⁵¹ developed $(n_1 + \dots + n_\omega)^m$, replaced each multinomial coefficient by unity, and denoted the result by $A[n_1 + \dots + n_\omega]^m$. Thus $A[n_1 + n_2]^2 = n_1^2 + n_1 n_2 + n_2^2$. Set $N_\omega = n_1 + \dots + n_\omega$. Then (pp. 65-9),

$$(1) \quad A[N_\omega - n_p]^m - A[N_\omega - n_q]^m = (n_q - n_p)A[N_\omega]^{m-1} \equiv 0 \pmod{n_q - n_p}.$$

Let $(n_1 \dots n_\omega)_m$ be the sum of the products of n_1, \dots, n_ω taken m at a time. Then (p. 143), if $A[N_\omega]^0 = 1$,

$$(2) \quad A[N_\omega]^\mu = (n_1 \dots n_\omega)_1 A[N_\omega]^{\mu-1} - (n_1 \dots n_\omega)_2 A[N_\omega]^{\mu-2} \\ + (n_1 \dots n_\omega)_3 A[N_\omega]^{\mu-3} - \dots + (-1)^{\mu+1} (n_1 \dots n_\omega)_\mu A[N_\omega]^0.$$

He discussed (pp. 146-151) in an obscure manner the solution of $X_1 \equiv X_2 \pmod{X}$, where the X 's are polynomials in ξ of degree ν . Set $N_\omega = n_1 + \dots + n_{\omega-2} + n_p + n_q$. Let the negatives of $n_1, \dots, n_{\omega-2}, n_p$ be the roots of $P = P_0 + P_1 x + \dots + P_{\omega-2} x^{\omega-2} + x^{\omega-1} = 0$; the negatives of $n_1, \dots, n_{\omega-2}, n_q$ the roots of $Q = Q_0 + \dots + x^{\omega-1} = 0$. We may add $\zeta_1 X$ and $\zeta_2 X$ to the members of our congruence. It is stated that the new first member may be taken to be $A[N_\omega - n_q]^m$, whence by (2)

$$X_1 + \zeta_1 X = P_{\omega-2} A[N_\omega - n_q]^{m-1} - P_{\omega-3} A[N_\omega - n_q]^{m-2} + \dots,$$

and the A 's may be expressed in terms of the P 's by (2). Similarly, $X_2 + \zeta_2 X$ may be expressed in terms of the Q 's. By (1), $X = n_q - n_p = Q_{\omega-2} - P_{\omega-2}$. Since $P = 0$, $Q = 0$ have $\omega - 2$ roots in common, we have further conditions on the coefficients P_i, Q_i . It is argued that $\omega - 3$ of the latter

¹⁴⁸Oeuvres, 2, 209, letter to Frenicle, Oct. 18, 1640.

¹⁴⁹Oeuvres, 2, 220, letter to Mersenne, June 15, 1641.

¹⁵⁰Mém. Ac. Sc. Paris, 1785, 483.

¹⁵¹Introduction à la Philosophie des Mathématiques et Technie de l'Arithmétique, Paris, 1811.

He used the Hebrew alphabet for the A of this report. Cf. Wronski¹⁶⁹ of Ch. VII.

remain arbitrary, and that ξ is a function of them and one of the n 's, which has an arbitrary rational value.

A. Cauchy¹⁵² noted that if f and F are polynomials in x , Lagrange's interpolation formula leads to polynomials u and v such that $uf + vF = R$, where R is a constant [provided f and F have no common factor]. If the coefficients are all integers, R is an integer. Hence R is the greatest of the integers dividing both f and F . For $f = x^p - x$, we may express R as a product of trigonometric functions. If also $F(x) = (x^n + 1)/(x + 1)$, where n and p are primes, $R = 0$ or ± 2 according as p is or is not of the form $nx + 1$. Hence the latter primes are the only ones dividing $x^n + 1$, but not $x + 1$.

Cauchy¹⁵³ proved that a congruence $f(x) \equiv 0 \pmod{p}$ of degree $m < p$ is equivalent to $(x - r)^i \phi(x) \equiv 0$, where ϕ is of degree $m - i$, if and only if

$$f(r) \equiv 0, \quad f'(r) \equiv 0, \dots, \quad f^{(i-1)}(r) \equiv 0 \pmod{p},$$

where p is a prime. The theorem fails if $m \geq p$. He gave the method of Libri (*Mémoires*, I) for solving the problem: Given $f(x) \equiv 0 \pmod{p}$ of degree $m \leq p$ and with exactly m roots, and $f_1(x)$ of degree $l \leq m$, to find a polynomial $\phi(x)$, also with integral coefficients, whose roots are the roots common to f and f_1 . He gave the usual theorem on the number of roots of a binomial congruence and noted conditions that a quartic congruence have four roots.

Cauchy¹⁵⁴ stated that if I is an arbitrary modulus and if r_1, \dots, r_m are roots of $f(x) \equiv 0 \pmod{I}$ such that each difference $r_i - r_j$ is prime to I , then

$$f(x) \equiv (x - r_1) \dots (x - r_m) Q(x) \pmod{I}.$$

If in addition, m exceeds the degree of $f(x)$, then $f(x) \equiv 0 \pmod{I}$ for every x . A congruence of degree n modulo p^λ , where p is a prime, has at most n roots unless every integer is a root. If $f(r) \equiv 0 \pmod{I}$ and if in the irreducible fraction equal to

$$\tau = \frac{f(r)}{If'(r)}$$

the denominator is prime to I , then $r - \tau I$ is a root of $f(x) \equiv 0 \pmod{I^2}$.

V. A. Lebesgue¹⁵⁵ wrote $a/b \equiv c \pmod{p}$ if b is prime to p and $a \equiv bc \pmod{p}$, and $a/b \equiv c/d \pmod{p}$ if b, d are prime to p and $ad \equiv bc \pmod{p}$.

J. A. Serret¹⁵⁶ stated and A. Genocchi proved that, if p is a prime, the sum of the m th powers of the p^n polynomials in x , of degree $n - 1$ and with integral coefficients $< p$, is a multiple of p if $m < p^n - 1$, but not if $m = p^n - 1$.

J. A. Serret¹⁵⁷ noted that all the real roots of a congruence $f(x) \equiv 0 \pmod{p}$, where p is a prime, satisfy $\psi(x) \equiv 0$, where ψ is the g. c. d. of $f(x)$ and $x^{p-1} - 1$.

¹⁵²Exercices de Math., 1, 1826, 160-6; Bull. Soc. Philomatique; Oeuvres, (2), 6, 202-8.

¹⁵³Exercices de Math., 4, 1829, 253-279; Oeuvres, (2), 9, 298-326.

¹⁵⁴Comptes Rendus Paris, 25, 1847, 37; Oeuvres, (1), 10, 324-30.

¹⁵⁵Nouv. Ann. Math., 9, 1850, 436.

¹⁵⁶Nouv. Ann. Math., 13, 1854, 314; 14, 1855, 241-5.

¹⁵⁷Cours d'algèbre supérieure, ed. 2, 1854, 321-3.

N. H. Abel¹⁵⁸ proved that we can solve by radicals any abelian equation, i. e., one whose roots are $r, \phi(r), \phi^2(r) = \phi[\phi(r)], \dots$, where ϕ is a rational function. H. J. S. Smith¹⁵⁹ concluded that when the roots of a congruence can be similarly expressed modulo p , its solution can evidently be reduced to the solution of binomial congruences, and the expressions for the roots of the corresponding equation may be interpreted as the roots of the congruence. For the special case $x^n \equiv 1$, this was done by Poincot in 1813–20 in papers discussed in the chapter on primitive roots.

M. Jenkins^{159a} noted that all solutions of $a^x \equiv 1 \pmod{x}$ are $x = U_n = u_1 u_2 \dots u_n$, where u_1 is any divisor of any power of $a-1$; u_2 any divisor prime to $a-1$, of any power of $a^{u_1}-1$; \dots ; u_n any divisor, prime to $a^{U_{n-2}}-1$, of any power of $a^{U_{n-1}}-1$. For $a^x + 1 \equiv 0 \pmod{x}$, modify the preceding by taking odd factors of $a+1$ instead of factors of $a-1$.

J. J. Sylvester¹⁶⁰ proved that if p is a prime and the congruence $f(x) \equiv 0 \pmod{p}$ of degree n has n real roots and if the resultant of $f(x)$ and $g(x)$ is divisible by p , then $g(x) \equiv 0$ has at least one root in common with $f(x) \equiv 0$. There are exactly $p-1$ real roots of $x^{p-1} \equiv 1 \pmod{p}$.

A. S. Hathaway¹⁶¹ noted the known similarity between equations and congruences for a prime modulus. He¹⁶² made abstruse remarks on higher congruences.

G. Frattini¹⁶³ proved that $x^2 - Dy^4 \equiv \lambda$ and $x^4 - Dy^2 \equiv \lambda$ are each solvable when the modulus is a prime $p > 5$ and $D \not\equiv 0$. If $d = B^2 - AC \not\equiv 0$, then $Ax^4 + 2Bx^2y + Cy^2 \equiv \lambda \pmod{p}$ is solvable since $dx^4 + \lambda C$ can be made congruent to a square and hence to $(Cy + Bx^2)^2$. Likewise for $ax^2 + 2bx + c \equiv y^4$.

A. Hurwitz¹⁶⁴ discussed the congruence of fractions and the theory of the congruence of infinite series. If $\phi(x) = r_0 + r_1x + \dots + r_n x^n/n! + \dots$ and if $\psi(x)$ is a similar series with the coefficients s_n , then ϕ and ψ are called congruent modulo m if and only if $r_n \equiv s_n \pmod{m}$ for $n = 1, 2, \dots$.

G. Cordone¹⁶⁵ treated the general quartic congruence for a prime modulus μ by means of a cubic resolvent. The method is similar to Euler's solution of a quartic equation as presented by Giudice in Peano's *Rivista di Matematica*, vol. 2. For the special case $x^4 + 6Hx^2 + K \equiv 0 \pmod{\mu}$, set $t = (\mu-1)/2$, $r^2 = 9H^2 - K$; then if K is a quadratic residue of μ , there are four rational roots or none according as $(-3H+r)^t \equiv +1$ or not; but if K is a non-residue, there are two rational roots or none according as one of the congruences

$$(-3H+r)^t \equiv +1, \quad (-3H-r)^t \equiv -1$$

is satisfied or not.

¹⁵⁸Jour. für Math., 4, 1829, 131; Oeuvres, 1, 114.

¹⁵⁹Report British Assoc. 1860, 120 seq., §66; Coll. M. Papers, 1, 141–5.

^{159a}Math. Quest. Educ. Times, 6, 1866, 91–3.

¹⁶⁰Amer. Jour. Math., 2, 1879, 360–1; Johns Hopkins University Circulars, 1, 1881, 131. Coll. Papers, 3, 320–1.

¹⁶¹Johns Hopkins Univ. Circulars, 1, 1881, 97.

¹⁶²Amer. Jour. Math., 6, 1884, 316–330.

¹⁶³Rendiconti Reale Accad. Lincei, Rome, (4), 1, 1885, 140–2.

¹⁶⁴Acta Mathematica, 19, 1895, 356.

¹⁶⁵Rendiconti Circolo Mat. di Palermo 9, 1895, 209–243.

R. Lipschitz¹⁶⁶ examined Fermat's¹⁴⁸ statement and proved that the primes p for which $a^x + 1 \equiv 0 \pmod{p}$ is impossible are those and only those for which a solution u of $u^{2^k} \equiv a \pmod{p}$ is a quadratic non-residue of p and for which $\lambda \leq k$, where 2^λ is the highest power of 2 dividing $p-1$. Cases when $a^x + 1 \equiv 0$ is impossible and not embraced by Fermat's rule are $a=2, p=89, 337$; $a=3, p=13$; $a=-2, p=281$; etc.

L. Kronecker¹⁶⁷ called $f(x)$ an invariant of the congruence $k \equiv k' \pmod{m}$, if the latter congruence implies the equality $f(k) = f(k')$. If also, conversely, the equality implies the congruence, $f(x)$ is called a proper (or characteristic) invariant, an example being the least positive residue of an integer modulo m . It is shown that every invariant of $k \equiv k' \pmod{m}$ can be represented as a symmetric function of all the integers congruent to k modulo m .

G. Wertheim¹⁶⁸ proved that $a^x + 1 \equiv 0 \pmod{p}$ is impossible if a belongs to an odd exponent modulo p [Fermat¹⁴⁸].

E. L. Bunitzky¹⁶⁹ (Bunickij) noted that, for any integer M , the congruences

$$f(a+kh) \equiv r_k \pmod{M} \quad (k=0, 1, \dots, n)$$

hold if and only if the coefficients A_k of $f(x)$ satisfy the conditions

$$k! h^k A_k \equiv \Delta^k r_0 \pmod{M} \quad (k=1, \dots, n).$$

If k is the least value of x for which $x! h^x$ is divisible by M , and if the g. c. d. of M and h is $k < m$, where m is a divisor of M , then if $f(x) \equiv 0 \pmod{M}$ has the roots $a, a+h, \dots, a+(k-1)h$, it has also the roots $a+jh$ ($j=k, k+1, \dots, m-1$).

G. Biase¹⁷⁰ called a similar to b in the ratio $m:n$ modulo k if the remainders on dividing a and b by k are in the ratio $m:n$. Two numbers similar to a third in two given ratios modulo k are similar to each other modulo k in a ratio equal to the quotient of the given ratios.

The problem¹⁷¹ to find n numbers whose n^2-n differences are incongruent modulo n^2-n+1 is possible for $n=6$, but not for $n=7$.

R. D. von Sterneck¹⁴⁰ proved that, if A is not divisible by the odd prime p , Ax^4+Bx^2+C takes $\psi(2AB, p)$ incongruent values (when x ranges over the set $0, 1, \dots, p-1$) if B is not divisible by p , while if B is divisible by p , it takes $(p+3)/4$ or $(p+1)/2$ values according as $p=4n+1$ or $p=4n-1$. In terms of Legendre's symbol,

$$\psi(a, p) = \frac{1}{8} \left[3p+4 - 2 \left(\frac{-2a}{p} \right) + \left(\frac{-1}{p} \right) + 2 \left(\frac{-a}{p} \right) \right].$$

¹⁶⁶Bull. des Sc. Math., (2), 22, I, 1898, 123-8. Extract in Oeuvres de Fermat, 4, 196-7.

¹⁶⁷Vorlesungen über Zahlentheorie, I, 1901, 131-142.

¹⁶⁸Anfangsgründe der Zahlenlehre, 1902, 265.

¹⁶⁹Zap. mat. otd. Obsc. (Soc. of natur.), Odessa, 20, 1902, III-VIII (in Russian); cf. Fortschr. Math., 33, 1902, p. 205.

¹⁷⁰Il Boll. Matematica Gior. Sc. Didat., Bologna, 4, 1905, 96.

¹⁷¹L'intermédiaire des math., 1906, 141; 1908, 64; 19, 1912, 130-1. Amer. Math. Monthly, 13, 1906, 215; 14, 1907, 107-8.

E. Landau¹⁷² proved that, if $f(x)=0$ is an equation with integral coefficients and at least one root of odd multiplicity, there exist an infinitude of primes $p=4n-1$ such that $f(x)\equiv 0 \pmod{p}$ has a root.

R. D. von Sterneck¹⁷³ found the number of combinations of the i th class (with or without repetition) of the numbers prime to p of a complete set of residues modulo p^x whose sum is congruent to a given integer modulo p^x , p being a prime.

E. Piccioli¹⁷⁴ gave known theorems on adding and multiplying congruences.

C. Jordan¹⁷⁵ found the number of sets of integers a_{ik} for which the determinant $|a_{ik}|$ of order n is congruent to a given integer modulo M .

C. Krediet¹⁷⁶ gave theorems on congruences of degree n for a prime modulus analogous to those for an algebraic equation of degree n , including the question of multiple roots. The determination of roots is often simplified by seeking first the roots which are quadratic residues and then those which are non-residues. The exposition is not clear or simple.

G. Rados¹⁷⁷ proved that, if p is a prime,

$$f(x)=a_0x^{p-2}+\dots+a_{p-2}\equiv 0, \quad g(x)=b_0x^{p-2}+\dots+b_{p-2}\equiv 0 \pmod{p}$$

have a common root if and only if each $R_i\equiv 0 \pmod{p}$, where

$$\Phi(u)=R_0u^{p-1}+R_1u^{p-2}+\dots+R_{p-1}$$

$$= \begin{vmatrix} a_0u+b_0 & a_1u+b_1 & \dots & a_{p-2}u+b_{p-2} \\ a_1u+b_1 & a_2u+b_2 & \dots & a_0u+b_0 \\ \dots & \dots & \dots & \dots \\ a_{p-2}u+b_{p-2} & a_0u+b_0 & \dots & a_{p-3}u+b_{p-3} \end{vmatrix}.$$

For $g=f'$, let $\Phi(u)$ become $D_0u^{p-2}+\dots+D_{p-2}$; thus $f(x)\equiv 0 \pmod{p}$ has a multiple root if and only if each $D_i\equiv 0 \pmod{p}$. Each of these theorems is extended to three congruences. Finally, if $f(x)$ and $f'(x)$ are relatively prime algebraically, there is only a finite number of primes p for which the number of roots of $f\equiv 0 \pmod{p^k}$ exceeds the degree of f .

G. Frattini¹⁷⁸ proved that if p and q are primes, q a divisor of $p-1$, every homogeneous symmetric congruence in q variables is solvable modulo p by values of the variables distinct from each other and from zero except when the degree of the congruence is divisible by q .

C. Grötsch¹⁷⁹ noted that if a is a root of $x^x\equiv a \pmod{p}$, where a is prime to p , then $x\equiv a \pmod{p^2-p}$ is a root, and proved that if θ is the g. c. d. of $\text{ind } a$ and $p-1$ and if $\text{ind } a > 0$, it has exactly

¹⁷²Handbuch... Verteilung der Primzahlen, 1, 1909, 440.

¹⁷³Sitzungsber. Ak. Wiss. Wien (Math.), 118, 1909, IIa, 119-132.

¹⁷⁴Il Pitagora, Palermo, 16, 1909-10, 125-7.

¹⁷⁵Jour. de Math., (6), 7, 1911, 409-416.

¹⁷⁶Wiskundig Tijdschrift, Haarlem, 7, 1911, 193-202 (Dutch).

¹⁷⁷Ann. sc. école norm. sup., (3), 30, 1913, 395-412.

¹⁷⁸Periodico di Mat., 29, 1913, 49-53.

¹⁷⁹Archiv Math. Phys., (3), 22, 1914, 49-53.

$$N = \phi(p-1) + \sum \delta \phi\left(\frac{p-1}{\delta}\right)$$

roots incongruent modulo $p(p-1)$, where δ ranges over all divisors >1 of θ . If $\text{ind } a = 0$, the number of such roots is $p-1+N$, where now δ ranges over the divisors >1 of $p-1$.

A. Châtelet¹⁸⁰ noted that divergences between congruences and equations are removed by not limiting attention to the given congruence $f(x) \equiv 0$ of degree n , but considering simultaneously all the polynomials $g(x)$ derived from $f(x)$ by a Tschirnhausen transformation $ky = \phi(x)$, where k is an integer and ϕ has integral coefficients and is of degree $n-1$.

*M. Tihanyi^{180a} proved a simple congruence.

R. Kantor¹⁸¹ discussed the number of incongruent values modulo m taken by a polynomial in n variables, and especially for $ax^3 + \dots + d$ modulo p^r , generalizing von Sterneck.¹⁴⁰

The solvability of $x^3 + 9x + 6 \equiv 0$ and $x^3 + y(y+1) \equiv 0 \pmod{p}$ has been treated.¹⁸²

A. Cunningham¹⁸³ announced the completion, in conjunction with Woodall and Creak, of tables of least solutions (x, a) of the congruences

$$r^x \equiv \pm y^a, \quad r^x y^a \equiv \pm 1 \pmod{p^k < 10000}, \quad r = 2, 10; y = 3, 5, 7, 11.$$

T. A. Pierce¹⁸⁴ gave two proofs that $f(x) \equiv 0 \pmod{p}$ has a real root if and only if the odd prime p divides $\Pi(1 - a_i^{p-1})$, where a_i ranges over the roots of the equation $f(x) = 0$.

Christie¹⁸⁵ stated that $t^p(t^p+1) \equiv 1 \pmod{p}$ if $t = 2 \sin 18^\circ$ and p is any odd prime. Cunningham gave a proof and a generalization.

*G. Rados¹⁸⁶ found the congruence of degree r having as its roots the r distinct roots $\neq 0$ of a given congruence of degree $p-2$ modulo p , a prime.

¹⁸⁰Comptes Rendus Paris, 158, 1914, 250-3.

^{180a}Math. és Phys. Lapok, Budapest, 23, 1914, 57-60.

¹⁸¹Monatshefte Math. Phys., 26, 1915, 24-39.

¹⁸²Wiskundige Opgaven, 12, 1915, 211-2, 215-7.

¹⁸³Messenger Math., 45, 1915-6, 69.

¹⁸⁴Annals of Math., (2), 18, 1916, 53-64.

¹⁸⁵Math. Quest. Educ. Times, 71, 1899, 82-3.

¹⁸⁶Math. és Termés Értésítő, 33, 1915, 702-10.

CHAPTER IX.

DIVISIBILITY OF FACTORIALS AND MULTINOMIAL COEFFICIENTS.

HIGHEST POWER OF A PRIME DIVIDING $m!$.

Genty¹ noted that the highest power of 2 dividing $(2^n)!$ is 2^{2^n-1} , and the quotient is $3^{n-1}(5 \cdot 7)^{n-2}(9 \cdot 11 \cdot 13 \cdot 15)^{n-3}(17 \dots 31)^{n-4} \dots (2^n - 1)$. In general if $P = 2^{n_1} + 2^{n_2} + \dots + 2^{n_r}$, where the n 's decrease, the highest power of 2 dividing $P!$ is 2^{P-r} .

A. M. Legendre² proved that if p^μ is the highest power of the prime p which divides $m!$, and if $[x]$ denotes the greatest integer $\leq x$,

$$(1) \quad \mu = \left[\frac{m}{p} \right] + \left[\frac{m}{p^2} \right] + \left[\frac{m}{p^3} \right] + \dots = \frac{m-s}{p-1},$$

where $s = a_0 + \dots + a_n$ is the sum of the digits of m to the base p :

$$m = a_0 p^n + a_1 p^{n-1} + \dots + a_n \quad (0 \leq a_i < p).$$

Th. Bertram³ stated Legendre's result in an equivalent form.

H. Anton⁴ proved that, if $n = vp + a$, $a < p$, $v < p$, and p is a prime,

$$\frac{n!}{p^v} \equiv (p-1)^v a! v! \pmod{p},$$

while, if $v = v'p + a'$, $a' < p$, $v' < p$,

$$\frac{n!}{p^{v+v'}} \equiv (p-1)^{v+v'} a'! v! v'! \pmod{p}.$$

D. André⁵ stated that the highest power p^μ of the prime p dividing $n!$ is given explicitly by $\mu = \sum_{k=1}^{\infty} [n/p^k]$ and claimed that merely the method of finding μ had been given earlier. He applied this result to prove that the product of n consecutive integers is divisible by $n!$.

J. Neuberg⁶ determined the least integer m such that $m!$ is divisible by a given power of a prime, but overlooked exceptional cases.

L. Stickelberger⁷ and K. Hensel⁸ gave the formula [cf. Anton⁴].

$$(2) \quad \frac{m!}{p^\mu} \equiv (-1)^\mu a_0! a_1! \dots a_n! \pmod{p}.$$

F. de Brun⁹ wrote $g[u]$ for the exponent of the highest power of the prime p dividing u . He gave expressions for

$$\psi(n; k) = \prod_{j=1}^n j^k, \quad g[\psi(n; k)]$$

in terms of the functions $h(a; k) = 1^k + 2^k + \dots + a^k$. A special case gives (1).

¹Hist. et Mém. Ac. R. Sc. Inscript. et Belles Lettres de Toulouse, 3, 1788, 97-101 (read Dec. 4, 1783).

²Théorie des nombres, ed. 2, 1808, p. 8; ed. 3, 1830, I, p. 10.

³Einige Sätze aus der Zahlenlehre, Progr. Köln, Berlin, 1849, 18 pp.

⁴Archiv Math. Phys., 49, 1869, 298-9.

⁵Nouv. Ann. Math., (2), 13, 1874, 185.

⁶Mathesis, 7, 1887, 68-69. Cf. A. J. Kempner, Amer. Math. Monthly, 25, 1918, 204-10.

⁷Math. Annalen, 37, 1890, 321.

⁸Archiv Math. Phys., (3), 2, 1902, 294.

⁹Arkiv för Matematik, Astr., Fysik, 5, 1904, No. 25 (French).

R. D. Carmichael¹⁰ treated the problem to find m , given the prime p and $s = \sum a_i$, in Legendre's formula; a given solution m_2 leads to an infinitude of solutions $m_2 p^k$, k arbitrary. Again, to find m such that p^{m-t} is the highest power of $p > 2$ dividing $m!$, we have $m-t = (m-s)/(p-1)$, and see that m has a limited number of values; there is always at least one solution m .

Carmichael¹¹ used the notation $H\{y\}$ for the index of the highest power of the prime p dividing y , and evaluated

$$h = H\left\{\prod_{x=0}^{n-1} (xa+c)\right\},$$

where a, c are relatively prime positive integers. Set $c_0 = c$ and let i_r be the least integer such that $i_r a + c_{r-1}$ is divisible by p , the quotient being c_r . Let

$$e_1 = \left\lfloor \frac{n-1-i_1}{p} \right\rfloor, \quad e_r = \left\lfloor \frac{e_{r-1}-i_r}{p} \right\rfloor, \quad r > 1.$$

Then $h = \sum_{r=1}^{t-1} (e_r + 1)$, where t is the least subscript for which

$$c_t(a+c_t)(2a+c_t) \dots (e_t a + c_t)$$

is not divisible by p . It follows that

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots \leq h \leq \left\lfloor \frac{n-1}{p} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \dots + R,$$

where R is the index of the highest power of p not exceeding $n-1$. If n is a power of p , $h = (n-1)/(p-1)$. But if $n = \delta_k p^k + \dots + \delta_1 p + \delta_0$, $\delta_k \neq 0$, and at least one further δ is not zero,

$$\frac{n-\sigma}{p-1} \leq h \leq k + \frac{n-\sigma}{p-1}, \quad \sigma = \delta_k + \dots + \delta_0.$$

In case the first x for which $xa+c$ is divisible by p gives c as the quotient, all the c_r are equal and hence all the i_r ; then

$$h = \left\lfloor \frac{n-1-i+p}{p} \right\rfloor + \left\lfloor \frac{n-1-i-ip+p^2}{p^2} \right\rfloor + \left\lfloor \frac{n-1-i-ip-ip^2+p^3}{p^3} \right\rfloor + \dots$$

The case $a=c=1$ yields Legendre's² result. The case $a=2, c=1$, gives

$$H\{1 \cdot 3 \cdot 5 \dots (2n-1)\} = \left\lfloor \frac{2n-1+p}{2p} \right\rfloor + \left\lfloor \frac{2n-1+p^2}{2p^2} \right\rfloor + \dots$$

E. Stridsberg¹² wrote H_m for (1) and considered

$$\pi_t = a(a+m) \dots (a+mt),$$

where a is any integer not divisible by the positive integer m . Let p be a prime not dividing m . Write a_j for the residue of aj modulo m . He noted that, if $pj \equiv 1 \pmod{m}$,

¹⁰Bull. Amer. Math. Soc., 14, 1907-8, 74-77; Amer. Math. Monthly, 15, 1908, 15-17.

¹¹*Ibid.*, 15, 1908-9, 217.

¹²Arkiv för Matematik, Astr., Fysik, 6, 1911, No. 34.

$$(p^{k+1}a_j^{k+1} - a)/m$$

is an integer, and wrote L_k for its residue modulo p^{k+1} . Set

$$t = \sum_{\nu=0}^k \tau_\nu p^\nu \quad (0 \leq \tau_\nu \leq p-1), \quad T_\mu = \sum_{\nu=0}^\mu \tau_\nu p^\nu \quad (\mu \leq k),$$

$$\Sigma_\mu = \left[\frac{p^{\mu+1} - 1 + T_\mu/L_\mu}{p^{\mu+1}} \right].$$

He proved that π_i is divisible by p^s , where $s = H_i + \sum_{\mu=0}^k \Sigma_\mu$. If τ_σ is the first one of the numbers τ_0, τ_1, \dots which is $< p-1$, π_i is divisible by p^σ ,

$$v = H_{i+1} + A_i, \quad 0 \leq A_i = \sum_{\mu=\sigma}^k \Sigma_\mu \leq k+1.$$

A. Cunningham¹³ proved that if z^ζ is the highest power of the prime z dividing p , the number of times p is a factor of $p^n!$ is the least of the numbers

$$\frac{p^n}{z^{\zeta n}} \cdot \frac{z^{\zeta n - \zeta + 1} - 1}{z - 1},$$

for the various primes z dividing p .

W. Jänichen¹⁴ stated and G. Szegö proved that

$$\Sigma \mu(n/d) \nu(d) = \phi(n)/(p-1),$$

summed for the divisors d of n , where $\nu(d)$ is the exponent of the highest power of p (a prime factor of n) which divides $d!$, for μ as in Ch. XIX.

INTEGRAL QUOTIENTS INVOLVING FACTORIALS.

Th. Schönemann¹⁵ proved, by use of symmetric functions of p th roots of unity, that if δ is the g. c. d. of μ, ν, \dots ,

$$\frac{\delta \cdot (m-1)!}{\mu! \nu! \dots} = \text{integer}, \quad (m = \mu + \nu + \dots).$$

He gave (p. 289) an arithmetical proof by showing that the fractions obtained by replacing δ by μ, ν, \dots are integers.

A. Cauchy¹⁶ proved the last theorem and that

$$\frac{(a+2b+\dots+nk) \cdot (m-1)!}{a! \dots k!} = \text{integer}, \quad (m = a + \dots + k).$$

D. André²⁰ noted that, except when $n=1, a=4, n(n+1) \dots (na-1)$ is not or is divisible by a^n according as a is a prime or not.

E. Catalan²¹ found by use of elliptic functions that

$$\frac{(m+n-1)!}{m!n!}, \quad \frac{(2m)!(2n)!}{m!n!(m+n)!}$$

are integers, provided m, n are relatively prime in the first fraction.

¹³L'intermédiaire des math., 19, 1912, 283-5. Text modified at suggestion of E. Maillet.

¹⁴Archiv Math. Phys., (3), 13, 1908, 361; 24, 1916, 86-7.

¹⁵Jour. für Math., 19, 1839, 231-243.

¹⁶Comptes Rendus Paris, 12, 1841, 705-7; Oeuvres, (1), 6, 109.

²⁰Nouv. Ann. Math., (2), 11, 1872, 314.

²¹Ibid., (2), 13, 1874, 207, 253. Arith. proofs, Amer. Math. Monthly, 18, 1911, 41-3.

P. Bachmann²² gave arithmetical proofs of Catalan's results.

D. André²³ proved that, if a_1, \dots, a_n have the sum N and if k of the a 's are not divisible by the integer >1 which divides the greatest number of the a 's, then $(N-k)!$ is divisible by $a_1! \dots a_n!$.

J. Bourguet²⁴ proved that, if $k \geq 2$,

$$\frac{(km_1)! (km_2)! \dots (km_k)!}{m_1! \dots m_k! (m_1 + \dots + m_k)!} = \text{integer}.$$

M. Weill²⁵ proved that the multinomial coefficient $(tq)! \div (q!)^t$ is divisible by $t!$.

Weill²⁶ stated that the following expression is an integer:

$$\frac{(a+\beta+\dots+pq+p_1q_1+\dots+rst)!}{a!\beta!\dots(p!)^q q! (p_1!)^{q_1} q_1! \dots (r!)^{st} (s!)^t t!}.$$

Weill²⁷ stated the special case that $(a+\beta+pq+rs)!$ is divisible by $a!\beta!(q!)^p p! (s!)^r r!$.

D. André²⁸ proved that $(tq)! \div (q!)^t$ is divisible by $(t!)^k$ if for every prime p the sum of the digits of q to base p is $\geq k$.

Ch. Hermite²⁹ proved that $n!$ divides

$$m(m+k)(m+2k) \dots \{m+(n-1)k\} k^{n-1}.$$

C. de Polignac³⁰ gave a simple proof of the theorem by Weill²⁵ and expressed the generalization by André²⁸ in another and more general form.

E. Catalan³¹ noted that, if s is the number of powers of 2 having the sum $a+b$,

$$\frac{(2a)! (2b)!}{a! b! (a+b)!}$$

is an even integer and the product of 2^s by an odd number.

E. Catalan³² noted that, if $n = a+b+\dots+t$,

$$\frac{n!(n+t)}{a! b! \dots t!}$$

is divisible by $a+t, b+t, \dots, a+b+t, \dots, a+b+c+t, \dots$.

E. Cesàro³³ stated and Neuberg proved that $\binom{n}{p}$ is divisible by $n(n-1)$ if p is prime to $n(n-1)$, and $p-1$ prime to $n-1$; and divisible by $(p+1) \times (p+2)$ if $p+1$ is prime to $n+1$, and $p+2$ is prime to $(n+1)(n+2)$.

²²Zeitschrift Math. Phys., 20, 1875, 161-3. Die Elemente der Zahlentheorie, 1892, 37-39.

²³Bull. Soc. Math. France, 1, 1875, 84.

²⁴Nouv. Ann. Math., (2), 14, 1875, 89; he wrote $\Gamma(n)$ incorrectly for $n!$; see p. 179.

²⁵Comptes Rendus Paris, 93, 1881, 1066; Mathesis, 2, 1882, 48; 4, 1884, 20; Lucas, Théorie des nombres, 1891, 365, ex. 3. Proof by induction, Amer. M. Monthly, 17, 1910, 147.

²⁶Bull. Soc. Math. France, 9, 1880-1, 172. Special case, Amer. M. Monthly, 23, 1916, 352-3.

²⁷Mathesis, 2, 1882, 48; proof by Liénard, 4, 1884, 20-23.

²⁸Comptes Rendus Paris, 94, 1882, 426.

²⁹Faculté des Sc. de Paris, Cours de Hermite, 1882, 138; ed. 3, 1887, 175; ed. 4, 1891, 196.

Cf. Catalan, Mém. Soc. Sc. de Liège, (2), 13, 1886, 262-4 (=Mélanges Math.); Heine.^{29a}

³⁰Comptes Rendus Paris, 96, 1883, 485-7. Cf. Bachmann, Niedere Zahlentheorie, I, 1902, 59-62.

³¹Atti Accad. Pont. Nouvi Lincei, 37, 1883-4, 110-3.

³²Mathesis, 3, 1883, 48; proof by Cesàro, p. 118.

³³Ibid., 5, 1885, 84.

E. Catalan³⁴ noted that

$$\binom{2n-2p}{n-p} \binom{2p}{p} \div \binom{n}{p} = \text{integer}.$$

F. Gomes Teixeira³⁵ discussed the result due to Weill.²⁶
De Presle³⁶ proved that

$$\frac{(k+1)(k+2)\dots(k+hl)}{l!(hl)!} = \text{integer},$$

being the product of an evident integer by $(hl)!/\{l!(hl)!\}$.

E. Catalan³⁷ noted that, if n is prime to 6,

$$\frac{(2n-4)!}{n!(n-2)!} = \text{integer}.$$

H. W. Lloyd Tanner³⁸ proved that

$$\frac{\{(\lambda_1 + \dots + \lambda_h)g\}!}{(\lambda_1! \dots \lambda_h!)^g (g!)^h} = \text{integer}.$$

L. Gegenbauer stated and J. A. Gmeiner³⁹ proved arithmetically that, if $n = \sum_{j=1}^r a_{j1} a_{j2} \dots a_{js}$, the product

$$m(m+k)(m+2k)\dots\{m+(n-1)k\}k^{n-r}$$

is divisible by

$$\prod_{j=1}^r \prod_{\nu=1}^s (a_{j\nu}!)^{a_{j\nu+1} \dots a_{js}},$$

where $m, k, n, a_{11}, \dots, a_{rs}$ are positive integers. This gives Hermite's²⁹ result by taking $r=s=1$. The case $m=k=1, s=2$, is included in the result by Weill.²⁶

Heine^{39a} and A. Thue⁴⁰ proved that a fraction, whose denominator is $k!$ and whose numerator is a product of k consecutive terms of an arithmetical progression, can always be reduced until the new denominator contains only such primes as divide the difference of the progression [a part of Hermite's²⁹ result].

F. Rogel⁴¹ noted that, if P be the product of the primes between $(p-1)/2$ and $p+1$, while n is any integer not divisible by the prime p ,

$$(n-1)(n-2)\dots(n-p+1)P/p \equiv 0 \pmod{P}.$$

S. Pincherle⁴² noted that, if n is a prime,

$$P = (x+1)(x+2)\dots(x+n-1)$$

is divisible by n and, if x is not divisible by n , by $n!$. If $n = \Pi p^a$, P is divisible

³⁴Nouv. Ann. Math., (3), 4, 1885, 487. Proof by Landau, (4), 1, 1901, 282.

³⁵Archiv Math. Phys., (2), 2, 1885, 265-8.

³⁶Bull. Soc. Math. France, 16, 1887-8, 159.

³⁷Mém. Soc. Roy. Sc. Liège, (2), 15, 1888, 111 (Mélanges Math. III). Mathesis, 9, 1889, 170.

³⁸Proc. London Math. Soc., 20, 1888-9, 287.

³⁹Monatshefte Math. Phys., 1, 1890, 159-162.

^{39a}Jour. für Math., 45, 1853, 287-8. Cf. Math. Quest. Educ. Times, 56, 1892, 62-63.

⁴⁰Archiv für Math. og Natur., Kristiania, 14, 1890, 247-250.

⁴¹Archiv Math. Phys., (2), 10, 1891, 93.

⁴²Rendiconto Sess. Accad. Sc. Istituto di Bologna, 1892-3, 17.

by $n!$ if and only if divisible by $\Pi p^{a+\beta}$, where β is the exponent of the power of p dividing $(n-1)!$.

G. Bauer⁴³ proved that the multinomial coefficient $(n+n_1+n_2+\dots)! \div \{n!n_1!\dots\}$ is an integer, and is even if two or more n 's are equal.

E. Landau⁴⁴ generalized most of the preceding results. For integers a_{ij} , b_{ij} , each ≥ 0 , and positive integers x_j , set

$$f = \frac{u_1! \dots u_m!}{v_1! \dots v_n!}, \quad u_i = \sum_{j=1}^r a_{ij} x_j, \quad v_i = \sum_{j=1}^r b_{ij} x_j.$$

Then f is an integer if and only if

$$\sum_{i=1}^m u_i \geq \sum_{i=1}^n v_i$$

for all real values of the x_j for which $0 \leq x_j \leq 1$. A new example is

$$\frac{(4m)!(4n)!}{m!n!(2m+n)!(m+2n)!} = \text{integer}.$$

P. A. MacMahon⁴⁵ treated the problem to find all a 's for which

$$\left(\frac{n+1}{1}\right)^{a_1} \left(\frac{n+2}{2}\right)^{a_2} \dots \left(\frac{n+m}{m}\right)^{a_m}$$

is an integer for all values of n ; in particular, to find those "ground forms" from which all the forms may be generated by multiplication. For $m=2$, the ground forms have $(a_1, a_2) = (1, 0)$ or $(1, 1)$. For $m=3$, the additional ground forms are $(1, 1, 1)$, $(1, 2, 1)$, $(1, 3, 1)$. For $m=4$, there are 3 new ground forms; for $m=5$, 13 new.

J. W. L. Glaisher⁴⁶ noted that, if $B_p(x)$ is Bernoulli's function, *i. e.*, the polynomial expression in x for $1^{p-1} + 2^{p-1} + \dots + (x-1)^{p-1}$ [Bernoulli^{150a} of Ch. V],

$$x(x+1) \dots (x+p-1)/p \equiv B_p(x) - x \pmod{p}.$$

He gave (*ibid.*, 33, 1901, 29) related congruences involving the left member and $B_{p-1}(x)$.

Glaisher⁴⁷ noted that, if r is not divisible by the odd prime p , and $l = kp + t$, $0 \leq t < p$,

$$l(r+l)(2r+l) \dots \{(p-1)r+l\}/p \equiv -\left\{\left[\frac{t}{p}\right]_r + k\right\} \pmod{p},$$

where $[t/p]_r$ denotes the least positive root of $px \equiv t \pmod{r}$. The residues mod p^3 of the same product $l(r+l) \dots$ are found to be complicated.

E. Maillet⁴⁸ gave a group of order $t!(q!)^t$ contained in the symmetric group on tq letters, whence follows Weill's²⁵ result.

⁴³Sitzungsber. Ak. Wiss. München (Math.), 24, 1894, 346-8.

⁴⁴Nouv. Ann. Math., (3), 19, 1900, 344-362, 576; (4), 1, 1901, 282; Archiv Math. Phys., (3), 1, 1901, 138. Correction, Landau.⁵³

⁴⁵Trans. Cambr. Phil. Soc., 18, 1900, 12-34.

⁴⁶Proc. London Math. Soc., 32, 1900, 172.

⁴⁷Messenger Math., 30, 1900-1, 71-92.

⁴⁸Mém. Prés. Ac. Sc. Paris, (2), 32, 1902, No. 8, p. 19.

M. Jenkins^{48a} counted in two ways the arrangements of $n = \phi f + \gamma g + \dots$ elements in ϕ cycles of f letters each, γ cycles of g letters, \dots , where f, g, \dots are distinct integers > 1 , and obtained the result

$$\frac{n!}{f^\phi \phi! g^\gamma \gamma! \dots} = n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots + (-1)^n \frac{1}{n!} \right).$$

C. de Polignac⁴⁹ investigated at length the highest power of $n!$ dividing $(nx)!/(x!)^n$. Let n_p be the sum of the digits of n to base p . Then

$$(x+n)_p = x_p + n_p - k(p-1), \quad (xn)_p = x_p \cdot n_p - k'(p-1),$$

where k is the number of units "carried" in making the addition $x+n$, and k' the corresponding number for the multiplication $x \cdot n$.

E. Schönbaum⁵⁰ gave a simplified exposition of Landau's first paper.⁴⁴

S. K. Maitra⁵¹ proved that $(n-1)(2n-1) \dots \{(n-2)n-1\}$ is divisible by $(n-1)!$ if and only if n is a prime.

E. Stridsberg⁵² gave a very elementary proof of Hermite's²⁹ result.

E. Landau⁵³ corrected an error in his⁴⁴ proof of the result in No. III of his paper, no use of which had been made elsewhere.

Birkeland¹⁸ of Ch. XI noted that a product of $2^p k$ consecutive odd integers is $\equiv 1 \pmod{2^p}$.

Among the proofs that binomial coefficients are integers may be cited those by:

G. W. Leibniz, *Math. Schriften*, pub. by C. I. Gerhardt, 7, 1863, 102.

B. Pascal, *Oeuvres*, 3, 1908, 278-282.

Gioachino Pessuti, *Memorie di Mat. Soc. Italiana*, 11, 1804, 446.

W. H. Miller, *Jour. für Math.*, 13, 1835, 257.

S. S. Greatheed, *Cambr. Math. Jour.*, 1, 1839, 102, 112.

Proofs that multinomial coefficients are integers were given by:

C. F. Gauss, *Disq. Arith.*, 1801, art. 41.

Lionnet, *Complément des éléments d'arith.*, Paris, 1857, 52.

V. A. Lebesgue, *Nouv. Ann. Math.*, (2), 1, 1862, 219, 254.

FACTORIALS DIVIDING THE PRODUCT OF DIFFERENCES OF r INTEGERS.

H. W. Segar⁶⁰ noted that the product of the differences of any r distinct integers is divisible by $(r-1)!(r-2)! \dots 2!$. For the special case of the integers $1, 2, \dots, n, r+1$, the theorem shows that the product of any n consecutive integers is divisible by $n!$.

A. Cayley⁶¹ used Segar's theorem to prove that

$$m(m-n) \dots (m-r-1n) \cdot n^r$$

is divisible by $r!$ if m, n are relatively prime [a part of Hermite's²⁹ result].

Segar⁶² gave another proof of his theorem. Applying it to the set

^{48a}*Quar. Jour. Math.*, 33, 1902, 174-9. ⁴⁹*Bull. Soc. Math. France*, 32, 1904, 5-43.

⁵⁰*Casopis*, Prag, 34, 1905, 265-300 (Bohemian).

⁵¹*Math. Quest. Educat. Times*, (2), 12, 1907, 84-5.

⁵²*Acta Math.*, 33, 1910, 243.

⁵³*Nouv. Ann. Math.*, (4), 13, 1913, 353-5.

⁶⁰*Messenger Math.*, 22, 1892-3, 59.

⁶¹*Messenger Math.* 22, 1892-3, p. 186. Cf. Hermite.²⁹

⁶²*Ibid.*, 23, 1893-4, 31. Results cited in *l'intermédiaire des math.*, 2, 1895, 132-3, 200; 5, 1898, 197; 8, 1901, 145.

$a, a+N, \dots, a+N^n$, we conclude that the product of their differences is divisible by $n!(n-1)!\dots 2!=\nu$. But the product equals

$$P = (N-1)^{n-1} (N^2-1)^{n-2} \dots (N^{n-2}-1)^2 (N^{n-1}-1),$$

multiplied by a power of N . Hence, if N is prime to $n!$, P is divisible by ν ; in any case a least number λ is found such that $N^\lambda P$ is divisible by ν . It is shown that the product of the differences of m_1, \dots, m_k is divisible by $k!(k-1)!\dots 2!$ if there be any integer p such that m_1+p, \dots, m_k+p are relatively prime to each of $1, 2, \dots, k$. It is proved that the product of any n distinct integers multiplied by the product of all their differences is a multiple of $n!(n-1)!\dots 2!$.

E. de Jonquières⁶³ and F. J. Studnička⁶⁴ proved the last theorem.

E. B. Elliott⁶⁵ proved Segar's theorem in the form: The product of the differences of n distinct numbers is divisible by the product of the differences of $0, 1, \dots, n-1$. He added the new theorems: The product of the differences of n distinct squares is divisible by the product of the differences of $0^2, 1^2, \dots, (n-1)^2$; that for the squares of n distinct odd numbers, multiplied by the product of the n numbers, is divisible by the product of the differences of the squares of the first n odd numbers, multiplied by their product.

RESIDUES OF MULTINOMIAL COEFFICIENTS.

Leibniz^{4, 7} of Ch. III noted that the coefficients in $(\Sigma a)^p - \Sigma a^p$ are divisible by p .

Ch. Babbage⁶⁹ proved that, if n is a prime, $\binom{2n-1}{n-1} - 1$ is divisible by n^2 , while $\binom{p+n}{p} - 1$ is divisible by p if and only if p is a prime.

G. Libri⁷⁰ noted that, if $m=6p+1$ is a prime,

$$6p - \binom{6p}{3} 3 + \binom{6p}{5} 3^2 - \dots \equiv 0,$$

$$2^{6p-2} + 6p - 1 - \binom{6p-1}{3} 3 + \binom{6p-1}{5} 3^2 - \dots \equiv 0 \pmod{m}.$$

E. Kummer⁷¹ determined the highest power p^N of a prime p dividing

$$\frac{(A+B)!}{A! B!}, \quad A \equiv a_0 + a_1 p + \dots + a_l p^l, \quad B \equiv b_0 + b_1 p + \dots + b_l p^l,$$

where the a_i and b_i belong to the set $0, 1, \dots, p-1$. We may determine c_i in this set and $\epsilon_i = 0$ or 1 such that

$$(3) \quad a_0 + b_0 = \epsilon_0 p + c_0, \quad \epsilon_0 + a_1 + b_1 = \epsilon_1 p + c_1, \quad \epsilon_1 + a_2 + b_2 = \epsilon_2 p + c_2, \dots$$

Multiply the first equation by 1 , the second by p , the third by p^2 , etc., and add. Thus

$$A+B = c_0 + c_1 p + \dots + c_l p^l + \epsilon_l p^{l+1}.$$

⁶³Comptes Rendus Paris, 120, 1895, 408-10, 534-7.

⁶⁴Vestnik. Ceske Ak., 7, 1898, No. 3, 165 (Bohemian).

⁶⁵Messinger Math., 27, 1897-8, 12-15.

⁶⁹Edinburgh Phil. Jour., 1, 1819, 46.

⁷⁰Jour. für Math., 9, 1832, 73. Proofs by Stern, 12, 1834, 288.

⁷¹Ibid., 44, 1852, 115-6. Cayley, Math. Quest. Educ. Times, 10, 1868, 88-9.

Hence, by Legendre's formula (1),

$$(p-1)N = A + B - \gamma - \epsilon_l - (A - a) - (B - \beta), \quad a = \Sigma a_i, \quad \beta = \Sigma b_i, \quad \gamma = \Sigma c_i.$$

Insert the value of $a + \beta$ obtained by adding equations (3). Thus

$$N = \epsilon_0 + \epsilon_1 + \dots + \epsilon_l.$$

A. Genocchi⁷² proved that, if m is the sum of n integers a, b, \dots, k , each divisible by $p-1$, and if $m < p^n - 1$, then $m! \div \{a!b!\dots k!\}$ is divisible by the prime p .

J. Wolstenholme⁷³ proved that $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$ if n is a prime > 3 .

H. Anton⁴ (303-6) proved that if $n = vp + a$, $r = wp + b$, where a, b, v, w are all less than the prime p ,

$$\binom{n}{r} \equiv \binom{a}{b} \binom{v}{w}, \quad \frac{1}{p} \binom{n}{r} \equiv \frac{1}{p} \binom{p+a}{b} \binom{v-1}{w} v \pmod{p},$$

according as $a \geq b$ or $a < b$.

M. Jenkins^{73a} considered for an odd prime p the sum

$$\sigma_r = \Sigma \binom{(m+n)r}{mr+k(p-1)},$$

extended over all the integers k between $nr/(p-1)$ and $-mr/(p-1)$, inclusive, and proved that $\sigma_r \equiv \sigma_p \pmod{p}$ if the g. c. d. of $r, p-1$ equals that of $p, p-1$.

E. Catalan⁷⁴ noted that $\binom{p-1}{p-1} \equiv 1 \pmod{p}$, if p is a prime.

Ch. Hermite⁷⁵ proved by use of roots of unity that the odd prime p divides

$$\binom{2n+1}{p-1} + \binom{2n+1}{2p-2} + \binom{2n+1}{3p-3} + \dots$$

E. Lucas⁷⁶ noted that, if $m = pm_1 + \mu$, $n = pn_1 + \nu$, $\mu < p$, $\nu < p$, and p is a prime,

$$\binom{n}{m} \equiv \binom{n_1}{m_1} \binom{\nu}{\mu} \pmod{p}.$$

In general, if μ_1, μ_2, \dots denote the residues of m and the integers contained in the fractions $m/p, m/p^2, \dots$, while the ν 's are the residues of $n, [n/p], \dots$,

$$\binom{n}{m} \equiv \binom{\nu_1}{\mu_1} \binom{\nu_2}{\mu_2} \dots \pmod{p}.$$

E. Lucas⁷⁷ proved the preceding results and

$$\binom{p}{n} \equiv 0, \quad \binom{p-1}{n} \equiv (-1)^n, \quad \binom{p+1}{n} \equiv 0 \pmod{p},$$

according as n is between 0 and p , 0 and $p-1$, or 1 and p .

⁷²Nouv. Ann. Math., 14, 1855, 241-3.

⁷³Quar. Jour. Math., 5, 1862, 35-9. For mod. n^2 , Math. Quest. Educ. Times, (2), 3, 1903, 33.

^{73a}Math. Quest. Educ. Times, 12, 1869, 29.

⁷⁴Nouv. Corresp. Math., 1, 1874-5, 76.

⁷⁵Jour. für Math., 81, 1876, 94.

⁷⁶Bull. Soc. Math. France, 6, 1877-8, 52.

⁷⁷Amer. Jour. Math., 1, 1878, 229, 230. For the second, anon.⁴³ of Ch. III (in 1830).

J. Wolstenholme⁷⁸ noted that the highest power of 2 dividing $\binom{2m-1}{m}$ is $q-p-1$, where q is the sum of the digits of $2m-1$ to base 2, and 2^p is the highest power of 2 dividing m .

J. Petersen⁷⁹ proved by Legendre's formula that $\binom{a+b}{a}$ equals the product of the powers of all primes p , the exponent of p being $(t_a+t_b-t_{a+b}) \div (p-1)$, where t_a is the sum of the digits of a to base p .

E. Cesàro⁸⁰ treated Kummer's⁷¹ problem. He stated (Ex. 295) and Van den Broeck⁸¹ proved that the exponent of the highest power of the prime p dividing $\binom{2n}{n}$ is the number of odd integers among $[2n/p]$, $[2n/p^2]$, $[2n/p^3]$,

O. Schlömilch^{81a} stated in effect that $\binom{kn}{n+1}$ is divisible by n .

E. Catalan⁸² proved that if n is odd,

$$\binom{2n}{n} + 10 \binom{2n-2}{n-1} \equiv 0 \pmod{n+2}.$$

W. J. C. Sharp^{82a} noted that $(p+n)! - p!n!$ is divisible by p^2 , if p is a prime $> n$. This follows also from $\binom{p+n}{n} \equiv 1 \pmod{p}$ [Dickson⁹⁰].

L. Gegenbauer⁸³ noted that, if σ is any integer, τ one of the form $6s$ or $3s$ according as n is odd or even,

$$(\tau - \sigma) \binom{2n}{n} + 5\sigma \binom{2n-2}{n-1} \equiv 0 \pmod{n+2}.$$

The case n odd, $\sigma=2$, $\tau=3$, gives Catalan's result.

E. Catalan⁸⁴ proved Hermite's⁷⁵ theorem.

Ch. Hermite⁸⁵ stated that $\binom{m}{n}$ is divisible by $m-n+1$ if m is divisible by n ; by $(m-n+1)/\epsilon$ if ϵ is the g. c. d. of $m+1$ and n ; by m/δ , if δ is the g. c. d. of m , n .

E. Lucas⁸⁶ noted that, if $n \leq p-1$, $p-2$, $p-3$, respectively,

$$\begin{aligned} \binom{p-1}{n} &\equiv (-1)^n, & \binom{p-2}{n} &\equiv (-1)^n(n+1), \\ \binom{p-3}{n} &\equiv (-1)^n \frac{(n+1)(n+2)}{2} \pmod{p}, \end{aligned}$$

if p is a prime, and proved Hermite's⁷⁵ result (p. 506).

F. Rogel⁸⁷ proved Hermite's⁷⁵ theorem by use of Fermat's.

⁷⁸Jour. de math. élém. et spéc., 1877-81, ex. 360.

⁷⁹Tidsskrift for Math., (4), 6, 1882, 138-143.

⁸⁰Mathesis, 4, 1884, 109-110.

⁸¹*Ibid.*, 6, 1886, 179.

^{81a}Zeitschrift Math. Naturw. Unterricht, 17, 1886, 281.

⁸²Mém. Soc. Roy. Sc. de Liège, (2), 13, 1886, 237-241 (= Mélanges Math.). Mathesis, 10, 1890, 257-8.

^{82a}Math. Quest. Educ. Times, 49, 1888, 74.

⁸³Sitzungsber. Ak. Wiss. Wien (Math.), 98, 1889, IIa, 672.

⁸⁴Mém. Soc. Sc. Liège, (2), 15, 1888, 253-4 (Mélanges Math. III).

⁸⁵Jour. de math. spéciales, problems 257-8. Proofs by Catalan, *ibid.*, 1889, 19-22; 1891, 70; by G. B. Mathews, Math. Quest. Educ. Times, 52, 1890, 63; by H. J. Woodall, 57, 1892, 91.

⁸⁶Théorie des nombres, 1891, 420.

⁸⁷Archiv Math. Phys., (2), 11, 1892, 81-3.

C. Szily⁸⁸ noted that no prime $> 2a$ divides

$$\sum_{k=0}^a \binom{a}{k}^2,$$

and specified the intervals in which its prime factors occur.

F. Morley⁸⁹ proved that, if $p = 2n + 1$ is a prime, $\binom{2n}{n} - (-1)^n 2^{4n}$ is divisible by p^3 if $p > 3$. That it is divisible by p^2 was stated as an exercise in Mathews' *Theory of Numbers*, 1892, p. 318, Ex. 16.

L. E. Dickson⁹⁰ extended Kummer's⁷¹ results to a multinomial coefficient M and noted the useful corollary that it is not divisible by a given prime p if and only if the partition of m into m_1, \dots, m_t arises by the separate partition of each digit of m written to the base p into the corresponding digits of m_1, \dots, m_t . In this case he proved that

$$M \equiv \prod_{i=0}^n \frac{a_i!}{a_i^{(1)}! \dots a_i^{(t)}!} \pmod{p}, \quad m_k = a_0^{(k)} p^n + \dots + a_n^{(k)}.$$

This also follows from (2) and from

$$(x_1 + \dots + x_t)^m \equiv (x_1 + \dots + x_t)^{a_n} (x_1^p + \dots + x_t^p)^{a_{n-1}} \dots (x_1^{p^n} + \dots + x_t^{p^n})^{a_0} \pmod{p}.$$

F. Mertens⁹¹ considered a prime $p \leq n$, the highest powers p^π and 2^π of p and 2 which are $\leq n$, and set $n_a = [n/2^a]$. Then $n! \div \{n_1! n_2! \dots n_\pi!\}$ is divisible by Πp^π , where p ranges over all the primes p .

J. W. L. Glaisher⁹² gave Dickson's⁹⁰ result for the case of binomial coefficients. He considered (349-60) their residues modulo p^n , and proved (pp. 361-6) that if $(n)_r$ denotes the number of combinations of n things r at a time, $\Sigma(n)_r \equiv (j)_k \pmod{p}$, where p is any prime, n any integer $\equiv j \pmod{p-1}$, while the summation extends over all positive integers r , $r \leq n$, $r \equiv k \pmod{p-1}$, and j, k are any of the integers $1, \dots, p-1$. He evaluated $\Sigma[(n)_r \div p]$ when r is any number divisible by $p-1$, and $(n)_r$ is divisible by p , distinguishing three cases to obtain simple results.

Dickson⁹³ generalized Glaisher's⁹² theorem to multinomial coefficients: Let k be that one of the numbers $1, 2, \dots, p-1$ to which m is congruent modulo $p-1$, and let k_1, \dots, k_t be fixed numbers of that set such that $k_1 + \dots + k_t \equiv k \pmod{p-1}$. Then if p is a prime,

$$\sum_{m_1, \dots, m_t} (m_1, m_2, \dots, m_t) \equiv \begin{cases} (k_1, k_2, \dots, k_t) & \text{if } k_1 + \dots + k_t = k \\ 0 & \text{if } k_1 + \dots + k_t > k \end{cases} \pmod{p},$$

where

$$(m_1, \dots, m_t) = \frac{(m_1 + \dots + m_t)!}{m_1! \dots m_t!}.$$

The second of the two proofs given is much the simpler.

⁸⁸Nouv. Ann. Math., (3), 12, 1893, Exercices, p. 52.* Proof, (4), 16, 1916, 39-42.

⁸⁹Annals of Math., 9, 1895, 168-170.

⁹⁰Ibid., (1), 11, 1896-7, 75-6; Quart. Jour. Math., 33, 1902, 378-384.

⁹¹Sitzungsber. Ak. Wiss. Wien (Math.), 106, IIa, 1897, 255-6.

⁹²Quar. Jour. Math., 30, 1899, 150-6, 349-366.

⁹³Ibid., 33, 1902, 381-4.

Glaisher⁹⁴ discussed the residues modulo p^3 of binomial coefficients.

T. Hayashi⁹⁵ proved that if p is a prime and $\mu + \nu = p$,

$$\binom{rp + \mu + s - 1}{rp + s} \equiv (-1)^s \binom{\nu}{s}, \quad 0, 1 \pmod{p},$$

according as $0 < s \leq \nu$, $\nu < s < p$, or $s = 0$.

T. Hayashi⁹⁶ proved that, if l_0 is the least positive residue of l modulo p , and if $\nu = p - \mu$,

$$\binom{l + \mu - 1}{l} \equiv (-1)^{l_0} \binom{\nu}{l_0} \equiv \binom{\nu + l - 1}{l} + \binom{\nu + l - p - 1}{l - p} + \binom{\nu + l - 2p - 1}{l - 2p} + \dots$$

modulo p . Special cases of the first result had been given by Lucas.⁸⁶

A. Cunningham⁹⁷ proved that, if p is a prime,

$$\binom{p-1}{x} \equiv (-1)^x \pmod{p}, \quad \frac{1}{2} \binom{2p}{p} \equiv 1 \pmod{p^3, p > 3}.$$

B. Ram⁹⁸ noted that, if $\binom{n}{m}$, $m = 1, \dots, n-1$, have a common factor $a > 1$, then a is a prime and $n = a^r$. There is at most one prime $< n$ which does not divide $\Pi \binom{n}{m}$ for $m = 1, \dots, n-2$, and then only when $n+1 = qa^r$, where a is a prime and $q < a$. For $m = 0, 1, \dots, n$, the number of odd $\binom{n}{m}$ is always a power of 2.

P. Bachmann⁹⁹ proved that, if $h(p-1)$ is the greatest multiple $< k$ of $p-1$,

$$\binom{k}{p-1} + \binom{k}{2(p-1)} + \dots + \binom{k}{h(p-1)} \equiv 0 \pmod{p},$$

the case k odd being due to Hermite.⁷⁵

G. Fontené stated and L. Grosschmid¹⁰⁰ proved that

$$\binom{Pk}{P(p-1)} \equiv (-1)^k \pmod{p}, \quad P = p^a, a \geq 0.$$

A. Fleck¹⁰¹ proved that, if $0 \leq \rho < p$, $a + b \equiv 0 \pmod{p}$,

$$\sum_{k=0}^{\infty} \binom{m}{\rho + kp} a^{m-\rho-kp} b^{\rho+kp} \equiv 0 \pmod{p^e}, \quad e = \left[\frac{m-1}{p-1} \right].$$

N. Nielsen¹⁰² proved Bachmann's⁹⁹ result by use of Bernoulli numbers.

⁹⁴Quar. Jour. Math., 31, 1900, 110-124.

⁹⁵Jour. of the Physics School in Tokio, 10, 1901, 391-2; Abh. Geschichte Math. Wiss., 28, 1910, 26-28.

⁹⁶Archiv Math. Phys., (3), 5, 1903, 67-9.

⁹⁷Math. Quest. Educat. Times, (2), 12, 1907, 94-5.

⁹⁸Jour. of the Indian Math. Club, Madras, 1, 1909, 39-43.

⁹⁹Niedere Zahlentheorie, II, 1910, 46.

¹⁰⁰Nouv. Ann. Math., (4), 13, 1913, 521-4.

¹⁰¹Sitzungs. Berlin Math. Gesell., 13, 1913-4, 2-6. Cf. H. Kapferer, Archiv Math. Phys. (3), 23, 1915, 122.

¹⁰²Annali di mat., (3), 22, 1914, 253.

A. Fleck¹⁰³ proved that

$$\binom{a}{a} \binom{a+1}{a} \binom{a+2}{a} \dots \binom{p-1}{a} \equiv (-1)^{a(a+1)/2} \binom{a}{1} \binom{a}{2} \dots \binom{a}{a-1} \pmod{p}$$

if and only if p is a prime. The case $a=1$ is Wilson's theorem.

Guérin¹⁰⁴ asked if Wolstenholme's⁷³ result is new and added that

$$\binom{kp-1}{p-1} \equiv k-1 \pmod{p^3}, \quad p \text{ prime} > 3.$$

THE CONGRUENCE $1 \cdot 2 \cdot 3 \dots (p-1)/2 \equiv \pm 1 \pmod{p}$.

J. L. Lagrange¹¹⁰ noted that $p-1, p-2, \dots, (p+1)/2$ are congruent modulo p to $-1, -2, \dots, -(p-1)/2$, respectively, so that Wilson's theorem gives

$$(4) \quad \left(1 \cdot 2 \cdot 3 \dots \frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

For p a prime of the form $4n+3$, he noted that

$$(5) \quad 1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv \pm 1 \pmod{p}.$$

E. Waring¹¹¹ and an anonymous writer¹¹² derived (4) in the same manner.

G. L. Dirichlet¹¹³ noted that, since -1 is a non-residue of $p=4n+3$, the sign in (5) is $+$ or $-$, according as the left member is a quadratic residue or non-residue of p . Hence if m is the number of quadratic non-residues $< p/2$ of p ,

$$1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv (-1)^m \pmod{p}.$$

C. G. J. Jacobi¹¹⁴ observed that, for $p > 3$, m is of the same parity as N , where $2N-1 = (Q-P)/p$, P being the sum of the least positive quadratic residues of p , and Q that of the non-residues. Writing the quadratic residues in the form $\pm k$, $1 \leq k \leq \frac{1}{2}(p-1)$, let m be the number of negative terms $-k$, and $-T$ their sum. Since -1 is a non-residue, m is the number of non-residues $< \frac{1}{2}p$ and

$$\Sigma(\pm k) = Sp, \quad P = \Sigma(+k) + \Sigma(p-k) = mp + Sp,$$

$$P+Q = 1 + \dots + p-1 = \frac{p(p-1)}{2}, \quad 2N-1 = \frac{P+Q}{p} - \frac{2P}{p} = \frac{p-1}{2} - 2(m+S).$$

Since $p=4n+3$, $N=n+1-m-S$. But $n+1$ and S are of the same parity since

$$pS+2T = 1+2+\dots+\frac{1}{2}(p-1) = \frac{1}{8}(p^2-1) = (2n+1)(n+1).$$

¹⁰³Sitzungs. Berlin Math. Gesell., 15, 1915, 7-8.

¹⁰⁴L'intermédiaire des math., 23, 1916, 174.

¹¹⁰Nouv. Mém. Ac. Berlin, 2, 1773, année 1771, 125; Oeuvres, 3, 432.

¹¹¹Meditat. Algebr., 1770, 218; ed. 3, 1782, 380.

¹¹²Jour. für Math., 6, 1830, 105.

¹¹³Ibid., 3, 1828, 407-8; Werke, 1, 107. Cf. Lucas, Théorie des nombres, 438; l'intermédiaire des math., 7, 1900, 347.

¹¹⁴Ibid., 9, 1832, 189-92; Werke, 6, 240-4.

He stated empirically that N is the number of reduced forms $ay^2 + byz + cz^2$, $4ac - b^2 = p$ for b odd, $ac - \frac{1}{4}b^2 = p$ for b even, where $b < a$, $b < c$.

C. F. Arndt¹¹⁵ proved in two ways that the product of all integers relatively prime to $M = p^n$ or $2p^n$, and not exceeding $(M-1)/2$, is $\equiv \pm 1 \pmod{M}$, when p is a prime $4k+3$, the sign being $+$ or $-$ according as the number of residues $> M/2$ of M is even or odd. Again,

$$\{1 \cdot 3 \cdot 5 \cdot 7 \dots (p-2)\}^2 \equiv \pm 1 \pmod{p},$$

the sign being $+$ or $-$ according as the prime p is of the form $4n+3$ or $4n+1$. In the first case, $1 \cdot 3 \dots (p-2) \equiv \pm 1 \pmod{p}$.

L. Kronecker¹¹⁶ obtained, for Dirichlet's¹¹³ exponent m , the result $m \equiv \nu \pmod{2}$, where ν is the number of positive integers of the form $q^{4l+1}r^2$ in the set $p-2^2, p-4^2, p-6^2, \dots$, and q is a prime not dividing r . Liouville (p. 267) gave $m \equiv k + \nu'' \pmod{2}$, when $p = 8k+3$ and ν'' is the number of positive integers of the form $q^{4l+1}r^2$ in the set $p-4^2, p-8^2, p-12^2, \dots$.

J. Liouville¹¹⁷ gave the result $m \equiv \sigma + \tau \pmod{2}$, for the case $p = 8k+3$, where τ is the number of positive integers of the form $2q^{4l+1}r^2$ (q a prime not dividing r) in the set $p-1^2, p-3^2, p-5^2, \dots$, and σ is the number of equal or distinct primes $4g+1$ dividing b , where $p = a^2 + 2b^2$ (uniquely).

A. Korkine¹¹⁸ stated that, if $[x]$ is the greatest integer $\leq x$,

$$m \equiv \frac{p-3}{4} + \sum_{k=1}^{(p-3)/4} \left[\sqrt{pk} \right] \pmod{p}.$$

J. Franel¹¹⁹ proved the last result by use of Legendre's symbol and

$$(-1)^m \equiv \prod_{r=1}^{(p-1)/2} \left(\frac{r}{p} \right), \quad \left(\frac{r}{p} \right) = (-1)^\mu, \quad \mu \equiv \sum_{s=1}^{(p-1)/2} \left[\frac{rs}{p} \right] \pmod{2}.$$

M. Lerch¹²⁰ obtained Jacobi's¹¹⁴ result.

H. S. Vandiver^{120a} proved Dirichlet's¹¹³ result and that

$$m \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{j^2}{p} \right] \pmod{2}.$$

R. D. Carmichael¹²¹ noted that (4) holds if and only if p is a prime.

E. Malo¹²² considered the residue $\pm r$ of $1 \cdot 2 \dots (p-1)/2$ modulo p , where p is a prime $4m+1$, and $0 < r < p/2$. Thus $r^2 \equiv -1$. The numbers $2, 3, \dots, (p-1)/2$, with r excluded, may be paired so that the product of the two of a pair is $\equiv \pm 1 \pmod{p}$. If this sign is minus for k pairs, $1 \cdot 2 \dots (p-1)/2 \equiv (-1)^k r \pmod{p}$.

*J. Ouspensky gave a rule to find the sign in (5).

OTHER CONGRUENCES INVOLVING FACTORIALS.

V. Bouniakowsky¹²⁹ noted that $(p-1)! = PP'$, $P \pm P' \equiv 0 \pmod{p}$ according as $p = 4k \mp 1$. For, if ρ is a primitive root of p , we may set $P = \rho\rho^2$

¹¹⁵Archiv Math. Phys., 2, 1842, 32, 34-35.

¹¹⁶Jour. de Math., (2), 5, 1860, 127.

¹¹⁷Ibid., 128.

¹¹⁸L'intermédiaire des math., 1, 1894, 95.

¹¹⁹Ibid., 2, 1895, 35-37.

¹²⁰Prag Sitzungsber. (Math.), 1898, No. 2.

^{120a}Amer. Math. Monthly, 11, 1904, 51-6.

¹²¹Ibid., 12, 1905, 106-8.

¹²²L'intermédiaire des math., 13, 1906, 131-2.

¹²³Bull. Soc. Phys. Math. Kasan, (2), 21.

¹²⁹Mém. Ac. Sc. St. Pétersbourg, (6), 1, 1831, 564.

$\dots \rho^t$, $P' = \rho^{t+1} \dots \rho^{p-1}$ with $t = (p-1)/2$, when $p = 4k-1$; but $P = \rho p^{p-1}$
 $\rho^3 \rho^{p-3} \dots$, $P' = \rho^2 \rho^{p-2} \rho^4 \rho^{p-4} \dots$, when $p = 4k+1$.

G. Oltramare¹³⁰ gave several algebraic series for the reciprocal of the binomial coefficient $\binom{2m}{m}$ and concluded that, if the moduli are primes,

$$1 + (m!)^4 \equiv -2 \left\{ \left(\frac{1}{3} \right)^2 + \left(\frac{1 \cdot 5}{3 \cdot 7} \right)^2 + \left(\frac{1 \cdot 5 \cdot 9}{3 \cdot 7 \cdot 11} \right)^2 + \dots \right\} \pmod{4m+1},$$

$$2^5 + (m!)^4 \equiv -2^6 \left\{ \left(\frac{3}{1} \right)^2 + \left(\frac{3 \cdot 7}{1 \cdot 5} \right)^2 + \left(\frac{3 \cdot 7 \cdot 11}{1 \cdot 5 \cdot 9} \right)^2 + \dots \right\} \pmod{4m+3}.$$

V. Bouniakowsky¹³¹ considered the integers q_1, \dots, q_s , each $< N$ and prime to N , arranged in ascending order of magnitude. If λ is any chosen integer $\leq s$, multiply

$$q_s = N - q_1, \quad q_{s-1} = N - q_2, \dots, \quad q_{s-\lambda+1} = N - q_\lambda$$

together and multiply the resulting equation by $q_1 \dots q_{s-\lambda}$. Apply the generalized Wilson theorem $q_1 \dots q_s + (-1)^s \equiv 0 \pmod{N}$. Hence

$$q_1 q_2 \dots q_\lambda q_1 q_2 \dots q_{s-\lambda} + (-1)^{s+\lambda} \equiv 0 \pmod{N}.$$

For N a prime, we have $s = N-1$ and

$$\lambda!(N-1-\lambda)! + (-1)^\lambda \equiv 0 \pmod{N} \quad (1 \leq \lambda \leq N-1).$$

C. A. Laisant and E. Beaujeux¹³² gave the last result and

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}, \quad k = \frac{p-1}{2}.$$

F. G. Teixeira¹³³ proved that if $a = 2^{2p-1}p - a$, $a < 2p-1$,

$$a(a+1) \dots (a+2p-1) \equiv 3^2 \cdot 5^2 \dots (2p-1)^2 p \pmod{a+a+1+a+2+\dots+a+2p-1}.$$

Thus, for $p=3$, $a=1$, $a=95$,

$$95 \cdot 96 \cdot 97 \cdot 98 \cdot 99 \cdot 100 \equiv 3^2 \cdot 5^2 \cdot 3 \pmod{585 = 95 + \dots + 100}.$$

M. Vecchi¹³⁴ noted that the final formula by Bouniakowsky¹³¹ follows by induction. Taking $\lambda = (N-1)/2$, we get Lagrange's formula (4). From the latter, we get

$$\{3 \cdot 5 \cdot 7 \dots (2y-1)\}^2 \left\{ \left(\frac{p-2y-1}{2} \right)! \right\}^2 / 2^{2y} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

The case $y = (p-1)/2$ gives Arndt's¹¹⁵ result

$$(6) \quad \{3 \cdot 5 \cdot 7 \dots (p-2)\}^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Vecchi¹³⁵ proved that, if ν is the number of odd quadratic non-residues of a prime $p = 4n+3$, then $1 \cdot 3 \cdot 5 \dots (p-2) \equiv (-1)^\nu \pmod{p}$. If μ is the number of non-residues $< p/2$, $1 \cdot 3 \cdot 5 \dots (p-2) \equiv (-1)^{\mu+1/2(p-1)/2} \pmod{p}$.

¹³⁰Mém. de l'Institut Nat. Genevois, 4, 1856, 33-6.

¹³²Jornal de Sciencias Math. e Astr., 3, 1881, 105-115.

¹³¹Bull. Ac. Sc. St. Pétersbourg, 15, 1857, 202-5.

¹³⁴Periodico di Mat., 16, 1901, 22-4.

¹³³Nouv. Corresp. Math., 5, 1879, 156 (177).

¹³⁵*Ibid.*, 22, 1907, 285-8.

R. D. Carmichael¹²¹ proved that, if $a+1$ and $2a+1$ are both primes, $(a!)^4-1$ is divisible by $(a+1)(2a+1)$, and conversely.

A. Arévalo¹³⁶ proved (6) and Lucas⁷⁷ residues of binomial coefficients.

N. G. W. H. Beeger¹³⁷ proved that [if p is a prime]

$$(p-1)!+1 \equiv s-p+1 \pmod{p^2}, \quad s=1+2^{p-1}+\dots+(p-1)^{p-1}=ph_{p-1},$$

where h is a Bernoulli number defined by the symbolical equation $(h+1)^n = h^n$, $h_1=1/2$. By use of Adams^{137a} table of h_i , $i < 114$, it was verified that $p=5$, $p=13$ are the only $p < 114$ for which $(p-1)!+1 \equiv 0 \pmod{p^2}$.

T. E. Mason¹³⁸ and J. M. Child¹³⁹ noted that, if p is a prime > 3 ,

$$(np)! \equiv n!(p!)^n \pmod{p^{n+3}}.$$

N. Nielsen¹⁴⁰ proved that, if $p=2n+1$, $P=1 \cdot 3 \cdot 5 \dots (2n-1)$,

$$P^2 \equiv (-1)^n 2^{2n} (2n)! \pmod{p^2},$$

$$(-1)^n 2^{2n} P^2 \equiv 2^{2n} \cdot 3 \cdot 5 \dots (4n-1) \pmod{16n^2}.$$

If p is a prime > 3 , $P \equiv (-1)^n 2^{3n} n! \pmod{p^3}$. He gave the last result also elsewhere.¹⁴¹

C. I. Marks¹⁴² found the smallest integer x such that $2 \cdot 4 \dots (2n)x$ is divisible by $3 \cdot 5 \dots (2n-1)$.

¹³⁶Revista de la Sociedad Mat. Española, 2, 1913, 130-1.

¹³⁷Messenger Math., 43, 1913-4, 83-4.

^{137a}Jour. für Math., 85, 1878, 269-72.

¹³⁸Tôhoku Math. Jour., 5, 1914, 137.

¹³⁹Math. Quest. Educ. Times, 26, 1914, 19.

¹⁴⁰Annali di mat., (3), 22, 1914, 81-2.

¹⁴¹K. Danske Vidensk. Selsk. Skrifter, (7), 10 1913, 353.

¹⁴²Math. Quest. Educ. Times, 21, 1912, 84-6.

CHAPTER X.

SUM AND NUMBER OF DIVISORS.

The sum of the k th powers of the divisors of n will be designated $\sigma_k(n)$. Often $\sigma(n)$ will be used for $\sigma_1(n)$, and $\tau(n)$ for the number $\sigma_0(n)$ of the divisors of n ; also,

$$T(n) = \tau(1) + \tau(2) + \dots + \tau(n).$$

The early papers in which occur the formulas for $\tau(n)$ and $\sigma(n)$ were cited in Chapter II.

L. Euler^{1, 2, 3} applied to the theory of partitions the formula

$$(1) \quad p(x) \equiv \prod_{k=1}^{\infty} (1 - x^k) = s \equiv 1 - x - x^2 + x^5 + x^7 - x^{12} - \dots$$

Euler⁴ verified for $n < 300$ that

$$(2) \quad \sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \dots,$$

in which two successive plus signs alternate with two successive minus signs, while the differences of 1, 2, 5, 7, 12, ... are 1, 3, 2, 5, 3, 7, ..., the alternate ones being 1, 2, 3, 4, ... and the others being the successive odd numbers. He stated that (2) can be derived from (1).

Euler⁵ noted that the numbers subtracted from n in (2) are pentagonal numbers $(3x^2 - x)/2$ for positive and negative integers x , and that if $\sigma(n-n)$ occurs it is to be replaced by n . He was led to the law of the series s by multiplying together the earlier factors of $p(x)$, but had no proof at that time that $p=s$. Comparing the derivatives of the logarithms of p and s , he found for $-x dp/(p dx)$ the two expressions equated in

$$(3) \quad \sum_{n=1}^{\infty} \frac{nx^n}{1-x^n} = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + \dots}{s}.$$

He verified for a few terms that the expansion of the left member is

$$(4) \quad \sum_{n=1}^{\infty} x^n \sigma(n).$$

Multiplying the latter by the series s and equating the product to the numerator of the right member of (3), he obtained (2) from the coefficients of x^n .

Euler⁶ proved (1) by induction. To prove (2), multiply the left member of (3) by $-dx/x$ and integrate. He obtained $\log p(x)$ and hence $\log s$, and then (3) by differentiation.

¹Letter to D. Bernoulli, Jan. 28, 1741, *Corresp. Math. Phys.* (ed. Fuss), II, 1843, 467.

²Euler, *Introductio in Analysin Infinitorum*, 1748, I, ch. 16.

³Novi Comm. Ac. Petrop., 3, 1750-1, 125; *Comm. Arith.*, 1, 91.

⁴Letter to Goldbach, Apr. 1, 1747, *Corresp. Math. Phys.* (ed. Fuss), I, 1843, 407.

⁵Posth. paper of 1747, *Comm. Arith.*, 2, 639; *Opera postuma*, I, 1862, 76-84. *Novi Comm. Ac. Petrop.*, 5, ad annos 1754-5, 59-74; *Comm. Arith.*, 1, 146-154.

⁶Letter to Goldbach, June 9, 1750, *Corresp. Math. Phys.* (ed. Fuss), I, 1843, 521-4. *Novi Comm. Ac. Petrop.*, 5, 1754-5, 75-83; *Acta Ac. Petrop.*, 4 I, 1780, 47, 56; *Comm. Arith.*, 1, 234-8; 2, 105. Cf. Bachmann, *Die Analytische Zahlentheorie*, 1894, 13-29.

Material on (1) will be given in the chapter on partitions in Vol. II. J. H. Lambert,⁷ by expanding the terms by simple division, obtained

$$\sum_{n=1}^{\infty} \frac{x^n}{1-x^n} = x + 2x^2 + 2x^3 + 3x^4 + \dots,$$

in which the coefficient of x^n is $\tau(n)$. Similarly, he obtained (4) from the left member of (3).

E. Waring⁸ reproduced Euler's⁶ proof of (2).

E. Waring⁹ employed the identity

$$\prod_{k=1}^n (x^k - 1) \equiv x^b - x^{b-1} - x^{b-2} + x^{b-5} + x^{b-7} - \dots = A,$$

the coefficient of x^{b-v} , for $v \leq n$, being $(-1)^z$ if $v = (3z^2 \pm z)/2$ and zero if v is not of that form. If $m \leq n$, the sum of the m th powers of the roots of $A=0$ is $\sigma(m)$. Thus (2) follows from Newton's identities between the coefficients and sums of powers of the roots. He deduced

$$(5) \quad 1 - \frac{m(m-1)}{2} \sigma(2) + \frac{m(m-1)(m-2)}{3} \sigma(3) - \frac{m(m-1)(m-2)(m-3)}{4} \sigma(4) \\ + \dots + \frac{m(m-1)(m-2)(m-3)}{2 \cdot 2^2} \{\sigma(2)\}^2 - \dots = c \cdot m!,$$

where $c = \pm 1$ or 0 is the coefficient of x^{b-m} in series A . Let

$$\Pi(x^p - 1) = x^{b'} - x^{b'-1} - x^{b'-2} + x^{b'-4} + x^{b'-8} - \dots = A',$$

where p ranges over the primes 1, 2, 3, 5, ..., n . If $m \leq n$, the sum of the m th powers of the roots of $A'=0$ equals the sum $\sigma'(m)$ of the prime divisors of m . Thus

$$\sigma'(m) = \sigma'(m-1) + \sigma'(m-2) - \sigma'(m-4) - \sigma'(m-8) + \sigma'(m-10) + \sigma'(m-11) \\ - \sigma'(m-12) - \sigma'(m-16) + \dots$$

We obtain (5) with σ replaced by σ' , and c by the coefficient of $x^{b'-m}$ in series A' . Consider

$$\prod_{j=1}^n (x^{jl} - 1) = x^b - x^{b-l} - x^{b-2l} + x^{b-5l} + \dots = B,$$

with coefficients as in series A . The sum of the (lm) th powers of the roots of $B=0$ equals the sum $\sigma^{(l)}(m)$ of those divisors of m which are multiples of l . Thus

$$\sigma^{(l)}(m) = \sigma^{(l)}(m-l) + \sigma^{(l)}(m-2l) - \sigma^{(l)}(m-5l) - \dots,$$

with the same laws as (2). The sum of those divisors of m which are divisible

⁷Anlage zur Architectonic, oder Theorie des Ersten und des Einfachen in der phil. und math. Erkenntniss, Riga, 1771, 507. Quoted by Glaisher.⁷⁶

⁸Meditationes Algebraicae, ed. 3, 1782, 345.

⁹Phil. Trans. Roy. Soc. London, 78, 1788, 388-394.

by the relatively prime numbers a, b, c, \dots is

$$\Sigma \sigma^{(a)}(m) - \Sigma \sigma^{(ab)}(m) + \Sigma \sigma^{(abc)}(m) - \dots$$

Waring noted that $\sigma(a\beta) = a\sigma(\beta) + (\text{sum of those divisors of } \beta \text{ which are not divisible by } a)$. Similarly,

$$\begin{aligned} \sigma(a\beta\gamma\dots) &= a\sigma(\beta\gamma\dots) + (\text{sum of divisors of } \beta\gamma\dots \text{ not divisible by } a) \\ &= a\beta\sigma(\gamma\delta\dots) + (\text{sum of divisors of } \beta\gamma\dots \text{ not divisible by } a) \\ &\quad + a(\text{sum of divisors of } \gamma\delta\dots \text{ not divisible by } \beta), \end{aligned}$$

etc. Again, $\sigma^{(l)}(a\beta) = a\sigma^{(l)}(\beta) + (\text{sum of divisors of } \beta \text{ divisible by } l \text{ but not by } a)$. The generalization is similar to that just given for σ .

C. G. J. Jacobi¹⁰ proved for the series s in (1) that

$$s^3 = 1 - 3x + 5x^3 - 7x^6 + \dots = \sum_{n=0}^{\infty} (-1)^n (2n+1) x^{n(n+1)/2}.$$

Jacobi¹¹ considered the excess $E(n)$ of the number of divisors of the form $4m+1$ of n over the number of divisors of the form $4m+3$ of n . If $n = 2^p uv$, where each prime factor of u is of the form $4m+1$ and each prime factor of v is of the form $4m+3$, he stated that $E(n) = 0$ unless v is a square, and then $E(n) = \tau(u)$.

Jacobi¹² proved the identity

$$(6) \quad (1+x+x^3+\dots+x^{k(k+1)/2}+\dots)^4 = 1 + \sigma(3)x + \dots + \sigma(2n+1)x^n + \dots$$

A. M. Legendre¹³ proved (1).

G. L. Dirichlet¹⁴ noted that the mean (mittlerer Werth) of $\sigma(n)$ is $\pi^2 n/6 - 1/2$, that of $\tau(n)$ is $\log n + 2C$, where C is Euler's constant 0.57721. . . . He stated the approximations to $T(n)$ and $\psi(n)$, proved later¹⁷, without obtaining the order of magnitude of the error.

Dirichlet¹⁵ expressed m in all ways as a product of a square by a complementary factor ϵ , denoted by ν the number of distinct primes dividing ϵ , and proved that $\Sigma 2^\nu = \tau(m)$.

Stern^{16a} proved (2) by expanding the logarithm of (1). If C'_n is the number of all combinations with repetitions with the sum n ,

$$\sigma(n) = nC'_n - C'_1\sigma(n-1) - C'_2\sigma(n-2) - \dots$$

Let $S(n)$ be the sum of the even divisors of n . Then, by (1),

$$S(2n) = S(2n-2) + S(2n-4) - S(2n-10) - S(2n-14) + \dots, \quad S(0) = 2n.$$

¹⁰Fundamenta Nova, 1829, § 66, (7); Werke, 1, 237. Jour. für Math., 21, 1840, 13; French transl., Jour. de Math, 7, 1842, 85; Werke, 6, 281. Cf. Bachmann,⁶ pp. 31-7.

¹¹Ibid., §40; Werke, 1, 1881, 163.

¹²Attributed to Jacobi by Bouniakowsky¹⁹ without reference. See Legendre (1828) and Plana (1863) in the chapter on polygonal numbers, vol. 2.

¹³Théorie des nombres, ed. 3, 1830, vol. 2, 128.

¹⁴Jour. für Math., 18, 1838, 273; Bericht Berlin Ak., 1838, 13-15; Werke, 1, 373, 351-6.

¹⁵Ibid., 21, 1840, 4. Zahlentheorie, § 124.

^{16a}Ibid., 177-192.

Let $S'(n)$ be the sum of the odd divisors of n , and C_n be the number of all combinations without repetitions with the sum n , so that $C_7 = 5$. Then

$$S'(n) = nC_n - S'(n-1)C_1 - S'(n-2)C_2 + \dots,$$

$$D(n) = -D(n-1) - D(n-3) - D(n-6) - \dots, \quad D(n) = S'(n) - S(n).$$

A complicated recursion formula for $\tau(n)$ is derived from

$$\log\{(1-x)(1-x^2)^{\frac{1}{2}}(1-x^3)^{\frac{1}{3}}\dots\} = -\sum_{n=1}^{\infty} \frac{1}{n} \tau(n) x^n.$$

Complicated recursion formulas are found for the number of integers $< m$ not factors of m , and for the sum of these integers. A recursion formula for the sum $s_r(n)$ of the divisors $\leq r$ of n is obtained by expanding

$$\log\{(1-x)(1-x^2)\dots(1-x^r)\} = -\sum_{n=1}^{\infty} \frac{1}{n} s_r(n) x^n.$$

Jacobi¹⁶ proved (1).

Dirichlet¹⁷ obtained approximations to $T(n)$. An integer $s \leq n$ occurs in as many terms of this sum as there are multiples of s among $1, 2, \dots, n$. The number of these multiples is $[n/s]$, the greatest integer $\leq n/s$. Hence

$$T(n) = \sum_{s=1}^n \left[\frac{n}{s} \right].$$

This sum is approximately the product of n by

$$\sum_{s=1}^n \frac{1}{s} = \log n + C + \frac{1}{2n} + \dots$$

Hence $T(n)$ is of the same order of magnitude as $n \log n$.

Let μ be the least integer $\geq \sqrt{n}$ and set $\nu = [n/\mu]$. Then if $g(x)$ is any function and $G(x) = g(1) + g(2) + \dots + g(x)$,

$$\sum_{s=1}^n \left[\frac{n}{s} \right] g(s) = -\nu G(\mu) + \sum_{s=1}^{\mu} \left[\frac{n}{s} \right] g(s) + \sum_{s=1}^{\nu} G\left\{ \left[\frac{n}{s} \right] \right\}.$$

In particular, if $g(x) = 1$,

$$T(n) = -\mu\nu + \sum_{s=1}^{\mu} \left[\frac{n}{s} \right] + \sum_{s=1}^{\nu} \left[\frac{n}{s} \right].$$

Giving to $[n/s]$ the approximation n/s , we see that

$$(7) \quad T(n) = n \log_e n + (2C-1)n + \epsilon,$$

where ϵ is of the same order of magnitude as \sqrt{n} .

Let $\rho(n)$ be the number of distinct prime factors > 1 of n . Then $2^{\rho(n)}$ is the number of ways of factoring n into two relatively prime factors, taking

¹⁶Jour. für Math., 32, 1846, 164; 37, 1848, 67, 73.

¹⁷Abhand. Ak. Wiss. Berlin, 1849, Math., 69-83; Werke, 2, 49-66. French transl., Jour. de Math., (2), 1, 1856, 353-370.

account of the order of the factors. The number of pairs of relatively prime integers ξ, η for which $\xi\eta \leq n$ is therefore

$$\psi(n) = \sum_{j=1}^n 2^{\rho(j)}.$$

For the preceding C and $T(n)$, it is proved that

$$T(n) = \sum_{s=1}^t \psi \left[\frac{n}{s^2} \right], \quad t = [\sqrt{n}],$$

$$\psi(n) = \frac{6n}{\pi^2} \left(\log_e n + \frac{12C'}{\pi^2} + 2C - 1 \right) + m, \quad C' = \sum_{s=2}^{\infty} \frac{\log s}{s^2},$$

where m is of the order of magnitude of n^δ , $\delta > \gamma/2$, while γ is determined by $\sum s^{-\gamma} = 1$ ($s = 2$ to ∞). Moreover, $T(n)$ is the number of pairs of integers x, y for which $xy \leq n$. He noted that

$$\sigma(1) + \sigma(2) + \dots + \sigma(n) = \sum_{s=1}^n s \left[\frac{n}{s} \right]$$

and that the difference between this sum and $\pi^2 n^2/12$ is of an order of magnitude not exceeding $n \log_e n$.

G. H. Burhenne¹⁸ proved by use of infinite series that

$$\tau(n) = \frac{1}{n!} \sum_{k=1}^n f^{(n)}(0), \quad f(x) \equiv \frac{x^k}{1-x^k},$$

and then expressed the result as a trigonometric series.

V. Bouniakowsky¹⁹ changed x into x^8 in (6), multiplied the result by x^4 and obtained

$$(x^1 + x^3 + x^5 + \dots)^4 = x^4 + \sigma(3)x^{12} + \dots + \sigma(2m+1)x^{8m+4} + \dots$$

Thus every number $8m+4$ is a sum of four odd squares in $\sigma(2m+1)$ ways. By comparing coefficients in the logarithmic derivative, we get

$$(8) \quad (1^2 - \overline{2m+1})\sigma(2m+1) + (3^2 - \overline{2m-1})\sigma(2m-1) + (5^2 - \overline{2m-5})\sigma(2m-5) + \dots = 0,$$

in which the successive differences of the arguments of σ are 2, 4, 6, 8, For any integer N ,

$$(9) \quad (1^2 - N)\sigma(N) + (3^2 - \overline{N-1 \cdot 2})\sigma(N-1 \cdot 2) + (5^2 - \overline{N-2 \cdot 3})\sigma(N-2 \cdot 3) + \dots = 0,$$

where $\sigma(0)$, if it occurs, means $N/6$. It is proved (p. 269) by use of Jacobi's¹⁰ result for s^3 that

$$1 + x + x^3 + x^6 + \dots = \frac{p(x^2)^2}{p(x)} = (1+x)(1+x^2)(1+x^3) \dots \\ (1-x^2)(1-x^4)(1-x^6) \dots,$$

¹⁸Archiv Math. Phys., 19, 1852, 442-9.

¹⁹Mém. Ac. Sc. St. Pétersbourg (Sc. Math. Phys.), (6), 4, 1850, 259-295 (presented, 1848).
Extract in Bulletin, 7, 170 and 15, 1857, 267-9.

where the exponents in the series are triangular numbers. Hence if we count the number of ways in which n can be formed as a sum of different terms from 1, 2, 3, . . . together with different terms from 2, 4, 6, . . ., first taking an even number of the latter and second an odd number, the difference of the counts is 1 or 0 according as n is a triangular number or not. It is proved that

$$(10) \quad \sigma(n) + \{\sigma(2) - 4\sigma(1)\}\sigma(n-2) + \sigma(3)\sigma(n-4) + \{\sigma(4) - 4\sigma(2)\}\sigma(n-6) \\ + \sigma(5)\sigma(n-8) + \{\sigma(6) - 4\sigma(3)\}\sigma(n-10) + \dots = \frac{n+1}{8}\sigma(n+2).$$

The fact that the second member must be an integer is generalized as follows: for n odd, $\sigma(n)$ is even or odd according as n is not or is a square; for n even, $\sigma(n)$ is even if n is not a square or the double of a square, odd in the contrary case. Hence squares and their doubles are the only integers whose sums of divisors are odd.

V. Bouniakowsky²⁰ proved that $\sigma(N) \equiv 2 \pmod{4}$ only when $N = kc^2$ or $2kc^2$, where k is a prime $4l+1$ [corrected by Liouville³⁰].

V. A. Lebesgue²¹ denoted by $1 + A_1x + A_2x^2 + \dots$ the expansion of the m th power of $p(x)$, given by (1), and proved, by the method used by Euler for the case $m=1$, that

$$\sigma(n) + A_1\sigma(n-1) + A_2\sigma(n-2) + \dots + A_{n-1}\sigma(1) + nA_n/m = 0.$$

This recursion formula gives

$$A_1 = -m, \quad A_2 = \frac{m(m-3)}{1 \cdot 2}, \quad A_3 = \frac{-m(m-1)(m-8)}{1 \cdot 2 \cdot 3}, \quad \dots$$

The expression for A_k was not found.

E. Meissel²² proved that (cf. Dirichlet¹⁷)

$$(11) \quad T(n) = \sum_{j=1}^n \left[\frac{n}{j} \right] = 2 \sum_{j=1}^{\nu} \left[\frac{n}{j} \right] - \nu^2 \quad (\nu = [\sqrt{n}]).$$

J. Liouville²³ noted that by taking the derivative of the logarithm of each member of (6) we get the formula, equivalent to (8):

$$\Sigma \left\{ n - \frac{5m(m+1)}{2} \right\} \sigma(2n+1-m^2-m) = 0,$$

summed for $m=0, 1, \dots$, the argument of σ remaining ≥ 0 .

J. Liouville²⁴ stated that it is easily shown that

$$\Sigma d\sigma(d) = \Sigma \left(\frac{m}{d} \right)^2 \sigma(d),$$

²⁰Mém. Ac. Sc. St. Pétersbourg, (6), 5, 1853, 303-322.

²¹Nouv. Ann. Math., 12, 1853, 232-4.

²²Jour. für Math., 48, 1854, 306.

²³Jour. de Math., (2), 1, 1856, 349-350 (2, 1857, 412).

²⁴Ibid., (2), 2, 1857, 56; Nouv. Ann. Math., 16, 1857, 181; proof by J. J. Hemming, *ibid.*, (2), 4, 1865, 547.

where d ranges over the divisors of m . He proved (p. 411) that

$$\Sigma(-1)^{m/d}d = 2\sigma(m/2) - \sigma(m).$$

J. Liouville²⁵ stated without proof the following formulas, in which d ranges over all the divisors of m , while $\delta = m/d$:

$$\Sigma\sigma(d) = \Sigma\delta\tau(d), \quad \Sigma\phi(d)\tau(\delta) = \sigma(m), \quad \Sigma\theta(d)\tau(\delta) = \{\tau(m)\}^2,$$

$$\Sigma\sigma(d)\sigma(\delta) = \Sigma d\tau(d)\tau(\delta), \quad \Sigma\tau(d)\tau(\delta) = \Sigma' \left\{ \tau\left(\frac{m}{D^2}\right) \right\}^2,$$

where $\phi(d)$ is the number of integers $< d$ and prime to d , $\theta(d)$ is the number of decompositions of d into two relatively prime factors, and the accent on Σ denotes that the summation extends only over the square divisors D^2 of m . He gave (p. 184)

$$\Sigma\theta(d) = \tau(m^2), \quad \Sigma'\theta\left(\frac{m}{D^2}\right) = \tau(m),$$

the latter being implied in a result due to Dirichlet.¹⁵

Liouville²⁶ gave the formulas, numbered (a), . . . , (k) by him, in which $\lambda(m) = +1$ or -1 , according as the total number of equal or distinct prime factors of m is even or odd:

$$\begin{aligned} \Sigma\tau(d^{2\mu}) &= \tau(m)\tau(m^\mu), & \Sigma\tau(d^{2\mu})\tau(\delta) &= \Sigma\tau(d)\tau(d^\mu), & \Sigma\phi(\delta)\sigma(d) &= m\tau(m), \\ \Sigma\delta\sigma(d) &= \Sigma d\tau(d), & \Sigma\lambda(d) &= 1 \text{ or } 0, & \Sigma\lambda(d)\theta(d)\tau(\delta) &= 1 \text{ or } 0, \end{aligned}$$

according as m is or is not a square;

$$\begin{aligned} \Sigma\lambda(d)\theta(d)\tau(\delta^2) &= 1, & \Sigma\lambda(d)\theta(d) &= \lambda(m), & \Sigma\lambda(d)\theta(\delta) &= 1, \\ \Sigma\lambda(d)\theta(d)\theta(\delta) &= 0, & \Sigma\lambda(\delta)\sigma(d) &= m\Sigma'\frac{1}{D^2}. \end{aligned}$$

The number of square divisors D^2 of m is $\Sigma\lambda(d)\tau(\delta)$.

Liouville²⁷ gave the formulas, numbered I–XVIII by him:

$$\begin{aligned} \Sigma\tau(\delta^2)\phi(d) &= \Sigma\delta\theta(d), & \Sigma d\tau(\delta^2) &= \Sigma\theta(\delta)\sigma(d), \\ \Sigma\tau(\delta^2)\lambda(d) &= \tau(m), & \Sigma\{\tau(\delta)\}^2\lambda(d)\theta(d) &= \tau(m), \\ \Sigma\phi(d)\tau(\delta)\tau(\delta^\mu) &= \Sigma d\tau(\delta^{2\mu}), & \Sigma\theta(\delta)\tau(d)\tau(d^\mu) &= \Sigma\tau(\delta^2)\tau(d^{2\mu}), \\ \Sigma\tau(\delta^{2\mu})\sigma(d) &= \Sigma\delta\tau(d)\tau(d^\mu), & \Sigma'\phi(D)\tau\left(\frac{m}{D^2}\right) &= \Sigma'D\theta\left(\frac{m}{D^2}\right), \\ \Sigma'\theta(D)\tau\left(\frac{m}{D^2}\right) &= \Sigma'\tau(D^2)\theta\left(\frac{m}{D^2}\right), & \Sigma'\tau(D)\tau(D^\mu)\theta\left(\frac{m}{D^2}\right)\Sigma'\tau(D^{2\mu})\tau &= \left(\frac{m}{D^2}\right), \\ \Sigma\lambda(\delta)\tau(d)\tau(d^\mu) &= \Sigma'\tau\left(\frac{m^{2\mu}}{D^{4\mu}}\right), & \Sigma\lambda(d)\sigma(d) &= m\lambda(m)\Sigma'\frac{1}{D^2}, \end{aligned}$$

²⁵Jour. de Mathématiques, (2), 2, 1857, 141–4. “Sur quelques fonctions numériques,” 1st article.

Here Σabc denotes $\Sigma(abc)$.

²⁶*Ibid.*, 244–8, second article of his series.

²⁷*Ibid.*, 377–384, third article of his series.

$$\begin{aligned}\Sigma' \lambda(D) \tau \left(\frac{m}{D^2} \right) &= \Sigma'' \theta \left(\frac{m}{e^4} \right), & \Sigma \{ \theta(d) \}^\mu &= \tau(m^{2\mu}), \\ \Sigma \phi(\delta) \tau(d^{2\mu}) &= \Sigma \delta \{ \theta(d) \}^\mu, & \Sigma \{ \theta(d) \}^\mu \tau(\delta) &= \Sigma \tau(d^{2\mu}) = \tau(m) \tau(m^{2\mu-1}), \\ \Sigma \tau(d^{2\mu}) \theta(\delta) &= \Sigma \{ \theta(d) \}^\mu \tau(\delta^2), & \Sigma \tau(d^{2\mu}) \lambda(\delta) &= \Sigma' \left\{ \theta \left(\frac{m}{D^2} \right) \right\}^\mu\end{aligned}$$

where, in Σ'' , e ranges over the biquadrate divisors of m .

Liouville²⁸ gave the formula

$$\Sigma \{ \tau(d) \}^3 = \{ \Sigma \tau(d) \}^2,$$

which implies that if $2m$ (m odd) has no factor of the form $4\mu+3$ and if we find the number of decompositions of each of its even factors as a sum of two odd squares, the sum of the cubes of the numbers of decompositions found will equal the square of their sum. Thus, for $m=25$,

$$50 = 1^2 + 7^2 = 7^2 + 1^2 = 5^2 + 5^2, \quad 10 = 3^2 + 1^2 = 1^2 + 3^2, \quad 2 = 1 + 1,$$

whence $3^3 + 2^3 + 1^3 = 6^2$.

Liouville²⁹ stated that, if a, b, \dots are relatively prime in pairs,

$$\sigma_n(ab \dots) = \sigma_n(a) \sigma_n(b) \dots,$$

while if p, q, \dots are distinct primes,

$$\sigma_n(p^a q^b \dots) = \frac{p^{n(a+1)} - 1}{p^n - 1} \cdot \frac{q^{n(b+1)} - 1}{q^n - 1} \dots$$

He stated the formulas

$$\begin{aligned}\Sigma \sigma_\mu(d) \phi(\delta) &= m \sigma_{\mu-1}(m), & \Sigma d^\mu \sigma_\nu(\delta) &= \Sigma d^\nu \sigma_\mu(\delta), \\ \Sigma \lambda(d) \tau(d^2) \sigma_\mu(\delta) &= \Sigma d^\mu \tau(\delta) \lambda(\delta), & \Sigma d^\mu \sigma_\mu(\delta) &= \Sigma d^\mu \tau(d), \\ \Sigma d^\mu \sigma_\mu(d) &= \Sigma \delta^{2\mu} \sigma_\mu(d), & \Sigma d^\mu \sigma_{3\mu}(\delta) &= \Sigma d^\mu \sigma_{2\mu}(d), \\ \Sigma d^\mu \sigma_{\nu+i}(d) \sigma_\nu(\delta) &= \Sigma d^\nu \sigma_{\mu+i}(d) \sigma_\mu(\delta), & \Sigma \lambda(d) \sigma_\mu(\delta) &= \Sigma' \left(\frac{m}{D^2} \right)^\mu, \\ \Sigma \tau(d^{2\mu}) \sigma_\nu(\delta) &= \Sigma d^\nu \tau(\delta) \tau(\delta^\mu), & \Sigma \{ \theta(d) \}^\nu \sigma_\mu(\delta) &= \Sigma d^\mu \tau(\delta^{2\nu}),\end{aligned}$$

and various special cases of them. To the seventh of these Liouville³⁰ later gave several forms, one being the case $\rho=0$ of

$$\Sigma d^{\mu-\nu} \sigma_{\nu+r}(d) \sigma_{\mu+\rho}(\delta) = \Sigma d^{\mu-\nu} \sigma_{\nu+\rho}(d) \sigma_{\mu+r}(\delta),$$

and proved (p. 84) the known theorem that $\sigma(m)$ is odd if and only if m is a square or the double of a square [cf. Bouniakowsky,¹⁹ end]. He proved that $\sigma(N) \equiv 2 \pmod{4}$ if and only if N is the product of a prime $4\lambda+1$, raised to the power $4l+1$ ($l \geq 0$), by a square or by the double of a square not divis-

²⁸Jour. de Mathématique, (2), 2, 1857, 393-6; Comptes Rendus Paris, 44, 1857, 753.

²⁹Ibid., 425-432, fourth article of his series.

³⁰Ibid., (2), 3, 1858, 63.

ible by the prime $4\lambda + 1$. The condition given by Bouniakowsky²⁰ is necessary, but not sufficient. Also,

$$\sigma_3(m) = \sum_{j=1}^m \sigma(2j-1)\sigma(2m-2j+1) \quad (m \text{ odd}).$$

J. Liouville's series of 18 articles, "Sur quelques formules . . . utiles dans la théorie des nombres," in Jour. de Math., 1858-1865, involve the function σ_n , but will be reported on in volume II of this History in connection with sums of squares. A paper of 1860 by Kronecker will be considered in connection with one by Hermite.⁷⁰

C. Traub³¹ investigated the number $(N; M, t)$ of divisors T of N which are $\equiv t \pmod{M}$, where M is prime to t and N . Let a, b, \dots, l be the integers $< M$ and prime to M ; let them belong modulo M to the respective exponents a', b', \dots, l' ; let m be a common multiple of the latter. Since any prime factor of N is of the form $Mx + k$, where $k = a, \dots, l$, any T is congruent to

$$a^A b^B \dots l^L \equiv t \pmod{M}, \quad 0 \leq A < a', \dots, 0 \leq L < l'.$$

Let A', \dots, L' be one of the n sets of exponents satisfying these conditions. If P is a primitive m th root of unity, the function

$$\psi = \frac{1}{a' \dots l'} \Sigma P^e, \quad e = (A - A')am/a' + \dots + (L - L')\lambda m/l',$$

summed for all sets $0 \leq a < a', \dots, 0 \leq \lambda < l'$, has the property that $\psi = 1$ if $A \equiv A' \pmod{a'}, \dots, L \equiv L' \pmod{l'}$ simultaneously, while $\psi = 0$ in all other cases. Thus $(N; M, t) = \Sigma \Sigma \psi$, where one summation refers to the n sets mentioned, while the other refers to the various divisors T of N . This double sum is simplified.

[The properties found (pp. 278-294) for the set of residues modulo M of the products of powers of a, \dots, l may be deduced more simply from the modern theory of commutative groups.]

V. Bouniakowsky³² considered the series

$$\psi(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}, \quad \{\psi(x)\}^m = \sum_{n=1}^{\infty} \frac{z_{n,m}}{n^x}.$$

By forming the product of $\psi(x)^{m-1}$ by $\psi(x)$, he proved that $z_{n,2}$ is the number $N_0(n) = \tau(n)$ of the divisors of n , and $z_{n,m}$ equals

$$N_{m-2}(n) = \Sigma N_{m-3}(d),$$

where (and below) d ranges over the divisors of n . Also,

$$\psi(x)\psi(x-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^x}.$$

From $\psi(x)^i \psi(x-1)^j$ for $(i, j) = (2, 1), (2, 2), (1, 2)$, he derived the first and fourth formulas of Liouville's²⁵ first article and the fourth of his²⁶ second article. He extended these three formulas to sums of powers of the divisors

³¹Archiv Math. Phys., 37, 1861, 277-345.

³²Mém. Ac. Sc. St. Pétersbourg, (7), 4, 1862, No. 2, 35 pp.

and proved the second formula in Liouville's first article and the first two summation formulas of Liouville.²⁹ He proved

$$\Sigma \sigma(d) = \Sigma N_1(d) \phi\left(\frac{n}{d}\right),$$

$$\sum_{x=1}^{\sigma} \tau(2x-1) = 2\sigma-1 + \sum_{x=1}^k \left[\frac{\sigma-1-x}{2x+1} \right], \quad k = \left[\frac{\sigma-2}{3} \right],$$

$$\tau(2\sigma-1) = 2 + \eta + \sum_{x=1}^l \left\{ \left[\frac{\sigma-1-x}{2x+1} \right] - \left[\frac{\sigma-2-x}{2x+1} \right] \right\}, \quad l = \left[\frac{\sigma}{3} \right] - 1,$$

where $\eta = 1$ or 0 according as $2\sigma-1$ is divisible by 3 or not. The last two were later generalized by Gegenbauer.³⁰

E. Lionnet³³ proved the first two formulas of Liouville.²⁹

J. Liouville³⁴ noted that, if q is divisible by the prime a ,

$$\sigma_{\mu}(aq) + a^{\mu} \sigma_{\mu}\left(\frac{q}{a}\right) = (a^{\mu} + 1) \sigma_{\mu}(q).$$

C. Sardi³⁵ denoted by A_n the coefficient of x^n in Jacobi's¹⁰ series for s^3 , so that $A_n = 0$ unless n is a triangular number. From that series he got

$$\sum_p (-1)^p (2p+1) \sigma \{ n - p(p+1)/2 \} = (-1)^{(t+1)/2} t n / 3 \text{ or } 0 \quad (t = \sqrt{1+8n}),$$

according as n is or is not a triangular number, and

$$\frac{n}{3} A_n + A_{n-1} \sigma(1) + \dots + A_1 \sigma(n-1) + A_0 \sigma(n) = 0.$$

This recursion formula determines A_n in terms of the σ 's, or $\sigma(n)$ in terms of the A 's. In each case the values are expressed by means of determinants of order n .

M. A. Andreievsky³⁶ wrote $N_{4h \pm 1}$ for the number of the divisors of the form $4h \pm 1$ of $n = a^{\alpha} b^{\beta} \dots$, where a, b, \dots are distinct primes. We have

$$N_{4h+1} - N_{4h-1} = \Sigma \left(\frac{-1}{d} \right) = \sum_{a'=0}^{\alpha} \left(\frac{-1}{a} \right)^{a'} \cdot \sum_{\beta'=0}^{\beta} \left(\frac{-1}{b} \right)^{\beta'} \dots,$$

where d ranges over all the divisors of n and the symbols are Legendre's. Evidently

$$\sum_{a'=0}^{\alpha} \left(\frac{-1}{a} \right)^{a'} = a+1 \text{ if } a=4l+1, \\ = 0 \text{ or } 1 \text{ if } a=4l-1,$$

according as a is odd or even. Hence, if any prime factor $4l-1$ of n occurs to an odd power, we have $N_{4h+1} = N_{4h-1}$. Next, let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots q_1^{2\beta_1} q_2^{2\beta_2} \dots,$$

where each p_i is a prime of the form $4l+1$, each q_i of the form $4l-1$. Then

$$N_{4h+1} - N_{4h-1} = (a_1+1)(a_2+1) \dots = \tau\left(\frac{n}{D^2}\right), \quad D = q_1^{\beta_1} q_2^{\beta_2} \dots$$

²⁹Nouv. Ann. Math., (2), 7, 1868, 68-72.

³⁰Jour. de math., (2), 14, 1869, 263-4.

³³Giornale di Mat., 7, 1869, 112-5.

³⁶Mat. Sbornik (Math. Soc. Moscow), 6, 1872-3, 97-106 (Russian).

The sum of the N 's is $\tau(n) = \tau(D^2)\tau(n/D^2)$. Hence

$$\frac{N_{4h+1}}{N_{4h-1}} = \frac{\tau(D^2) + 1}{\tau(D^2) - 1},$$

which is never an integer other than 1 or 2 when n is odd. If it be 2, $\tau(D^2) = 3$ requires that D be a prime. Similarly, for Legendre's symbol $(2/a)$,

$$N_{8h+1} - N_{8h+3} = \sum_{a'=0}^a \left(\frac{2}{a}\right)^{a'} \cdot \sum_{\beta'=0}^{\beta} \left(\frac{2}{b}\right)^{\beta'} \dots$$

is zero if any prime factor $8l \pm 3$ of n occurs to an odd power, but is $\Pi (\alpha_i + 1)$ if in n each p_i is a prime $8l \pm 1$ and each q_i a prime $8l \pm 3$. For n odd, N_{8h+1}/N_{8h+3} can not be an integer other than 1 or 2; if 2, D is a prime.

F. Mertens³⁷ proved (11). He considered the number $\nu(n)$ of divisors of n which are not divisible by a square > 1 . Evidently $\nu(n) = 2^\rho$, where ρ is the number of distinct prime factors of n . If $\mu(n)$ is zero when n has a square factor > 1 and is $+1$ or -1 according as n is a product of an even or odd number of distinct primes, $\nu(n) = \sum \mu^2(d)$, where d ranges over the divisors of n . Also,

$$\sum_{k=1}^n \nu(k) = \sum_{k=1}^t \mu(k) T\left(\frac{n}{k^2}\right), \quad t = [\sqrt{n}].$$

He obtained Dirichlet's¹⁷ expression $\psi(n)$ for this sum, finding for m a limit depending on C and n , of the order of magnitude of $\sqrt{n} \log_e n$.

E. Catalan^{37a} noted that $\sum \sigma(i)\sigma(j) = 8\sigma_3(n)$ where $i+j=4n$. Also, if i is odd, $\sigma(i)$ equals the sum of the products two at a time of the E 's of the odd numbers whose sum is $2i$, where E denotes the excess of the number of divisors $4\mu+1$ over the number of divisors $4\mu-1$.

H. J. S. Smith³⁸ proved that, if $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots$,

$$\sigma_s(m) - \sum \sigma_s\left(\frac{m}{p_1}\right) + \sum \sigma_s\left(\frac{m}{p_1 p_2}\right) - \dots = m^s.$$

For, if $P = 1 + p^s + \dots + p^{as}$, $P' = 1 + p^s + \dots + p^{(a-1)s}$, then

$$\sigma_s(m) = P_1 P_2 \dots, \quad \sigma_s\left(\frac{m}{p_1}\right) = P_1' P_2 \dots, \quad \sigma_s\left(\frac{m}{p_1 p_2}\right) = P_1' P_2' P_3 \dots,$$

and the initial sum equals $(P_1 - P_1')(P_2 - P_2') \dots = m^s$.

J. W. L. Glaisher³⁹ stated that the excess of the sum of the reciprocals of the odd divisors of a number over that for the even divisors is equal to the sum of the reciprocals of the divisors whose complementary divisors are odd. The excess of the sum of the divisors whose complementary divisors are odd over that when they are even equals the sum of the odd divisors.

G. Halphen⁴⁰ obtained the recursion formula

$$\sigma(n) = 3\sigma(n-1) - 5\sigma(n-3) + \dots - (-1)^x (2x+1)\sigma\left\{n - \frac{x(x+1)}{2}\right\} + \dots,$$

³⁷Jour. für Math., 77, 1874, 291-4.

^{37a}Recherches sur quelques produits indéfinis, Mém. Ac. Roy. Belgique, 40, 1873, 61-191. Extract in Nouv. Ann. Math., (2), 13, 1874, 518-523.

³⁸Proc. London Math. Soc., 7, 1875-6, 211.

³⁹Messenger Math., 5, 1876, 52.

⁴⁰Bull. Soc. Math. France, 5, 1877, 158.

where, if n is of the form $x(x+1)/2$, $\sigma(0)$ is to be taken to be $n/3$ [Glaisher^{63, 67}]. The proof follows from the logarithmic derivative of Jacobi's¹⁰ expression for s^3 , as in Euler's⁶ proof of (2).

Halphen⁴¹ formed for an odd function $f(z)$ the sum of

$$(-1)^x f\left(\frac{a-x^2}{y} + x\right),$$

x taking all integral values between the two square roots of a , and y ranging over all positive odd divisors of $a-x^2$. This sum is

$$(-1)^{a+1} \sqrt{a} f(\sqrt{a})$$

if a is a square, zero if a is not a square. Taking $f(z) = z$, we get a recursion formula for the sum of those divisors d of x for which x/d is odd [see the topic Sums of Squares in Vol. II of this History]. Taking $f(z) = a^z - a^{-z}$, we get a recursion formula for the number of odd divisors $< a/m$ of a . A generalization of (2) gives a recursion formula for the sum of the divisors of the forms $2nk$, $n(2k+1) \pm m$, with fixed n, m .

E. Catalan⁴² denoted the square of (1) by $1 + L_1x + \dots + L_nx^n + \dots$. Thus

$$\sigma(n) + L_1\sigma(n-1) + L_2\sigma(n-2) + \dots + L_{n-1} = -\frac{n}{2}L_n,$$

$$L_n - L_{n-1} - L_{n-2} + L_{n-5} + L_{n-7} - \dots = 0 \text{ or } (2\lambda+1)(-1)^\lambda,$$

according as n is not or is of the form $\lambda(\lambda+1)/2$. In view of the equality of (3) and (4) and the fact that $1/p = \sum \psi(n)x^n$, where $\psi(n)$ is the number of partitions of n into equal or distinct positive integers, he concluded that

$$\sigma(n) = \psi(n-1) + 2\psi(n-2) - 5\psi(n-5) - 7\psi(n-7) + 12\psi(n-12) + \dots$$

J. W. L. Glaisher⁴³ noted that, if $\theta(n)$ is the excess of the sum of the odd divisors of n over the sum of the even divisors,

$$\theta(n) + \theta(n-1) + \theta(n-3) + \theta(n-6) + \dots = 0,$$

where 1, 3, 6, ... are the triangular numbers, and $\theta(n-n) = -n$.

E. Cesàro⁴⁴ denoted by s_n the sum of the residues obtained by dividing n by each integer $< n$, and stated that

$$s_n + \sigma(1) + \sigma(2) + \dots + \sigma(n) = n^2.$$

E. Catalan⁴⁵ proved the equivalent result that the sum of the divisors of $1, \dots, n$ equals the sum of the greatest multiples, not $> n$, of these numbers.

Catalan⁴⁶ stated that, if $\phi(a, n)$ is the greatest multiple $\leq n$ of a ,

$$\sigma(n) = \sum_{a=1}^n \{\phi(a, n) - \phi(a, n-1)\}.$$

⁴¹Bull. Soc. Math. France, 6, 1877-8, 119-120, 173-188.

⁴²Assoc. franç. avanc. sc., 6, 1877, 127-8. Cf. Catalan.^{37a}

⁴³Messenger Math., 7, 1877-8, 66-7.

⁴⁴Nouv. Corresp. Math., 4, 1878, 329; 5, 1879, 22; Nouv. Ann. Math., (3), 2, 1883, 289; 4, 1885, 473.

⁴⁵Ibid., 5, 1879, 296-8; stated, 4, 1879, ex. 447.

⁴⁶Ibid., 6, 1880, 192.

Radicke (p. 280) gave an easy proof and noted that if we take $n=1, \dots, m$ and add, we get the result by E. Lucas⁴⁷

$$\sigma(1) + \dots + \sigma(m) = \phi(1, m) + \dots + \phi(m, m).$$

J. W. L. Glaisher⁴⁸ stated that if $f(n)$ is the sum of the odd divisors of n and if $g(n)$ is the sum of the even divisors of n , and $f(0)=0$, $g(0)=n$, then

$$\begin{aligned} f(n) + f(n-1) + f(n-3) + f(n-6) + f(n-10) + \dots \\ = g(n) + g(n-1) + g(n-3) + \dots \end{aligned}$$

Chr. Zeller⁴⁹ proved (11).

R. Lipschitz⁵⁰ wrote $G(t)$ for $\sigma(1) + \dots + \sigma(t)$, $D(t)$ for $(t^2+t)/2$, and $\Phi(t)$ for $\phi(1) + \dots + \phi(t)$, using Euler's $\phi(t)$. Then if 2, 3, 5, 6, ... are the integers not divisible by a square >1 ,

$$\begin{aligned} T(n) - T\left[\frac{n}{2}\right] - T\left[\frac{n}{3}\right] - T\left[\frac{n}{5}\right] + \dots &= n, \\ G(n) - 2G\left[\frac{n}{2}\right] - 3G\left[\frac{n}{3}\right] - 5G\left[\frac{n}{5}\right] + \dots &= n, \\ D(n) - D\left[\frac{n}{2}\right] - D\left[\frac{n}{3}\right] - D\left[\frac{n}{5}\right] + \dots &= \Phi(n), \end{aligned}$$

the sign depending on the number of prime factors of the denominator. He discussed (pp. 985-7) Dirichlet's¹⁷ results on the mean of $\tau(n)$, $\sigma(n)$, $\phi(n)$.

A. Berger⁵¹ proved by use of gamma functions that the mean of the sum of the divisors d of n is $\pi^2 n/6$, that of $\sum d/2^d$ is 1, that of $\sum 1/d$ is $\pi^2/6$.

G. Cantor^{51a} gave the second formula of Liouville²⁵ and his²⁶ third.

A. Piltz⁵² considered the number $T_k(n)$ of sets of positive integral solutions of $u_1 \dots u_k = n$, where differently arranged u 's give different sets. Thus $T_1(n) = 1$, $T_2(n) = \tau(n)$. If σ is the real part of the complex number s , and n^s denotes $e^{s \log n}$ for the real value of the logarithm, he proved that

$$t_k(x; s) = \sum_{n=1}^x \frac{T_k(n)}{n^s} = x^{1-s} \sum_{m=0}^k b_m \log^m x + b + O(x^l) + O(x^l \log^{k-2} x),$$

where $l = 1 - \sigma - 1/k$, and the b 's are constants, $b_k = 0$ for $s \neq 1$; while $O(f)$ is⁹⁰ of the order of magnitude of f . Taking $s=0$, we obtain the number $\sum T_k(n)$ of sets of positive integral solutions of $u_1 \dots u_k \leq x$.

H. Ahlborn⁵³ treated (11).

E. Cesàro⁵⁴ noted that the mean of the difference between the number of odd and number of even divisors of any integer is $\log 2$; the limit for

⁴⁷Nouv. Corresp. Math., 5, 1879, 296.

⁴⁸Nouv. Corresp. Math., 5, 1879, 176.

⁴⁹Göttingen Nachrichten, 1879, 265.

⁵⁰Comptes Rendus Paris, 89, 1879, 948-50. Cf. Bachmann²⁰ of Ch. XIX.

⁵¹Nova Acta Soc. Sc. Upsal., (3), 11, 1883, No. 1 (1880). Extract by Catalan in Nouv. Corresp. Math., 6, 1880, 551-2. Cf. Gram.^{64a}

^{51a}Göttingen Nachr., 1880, 161; Math. Ann., 16, 1880, 586.

⁵²Ueber das Gesetz, nach welchem die mittlere Darstellbarkeit der natürlichen Zahlen als Produkte einer gegebenen Anzahl Faktoren mit der Grösse der Zahlen wächst. Diss., Berlin, 1881.

⁵³Progr., Hamburg, 1881.

⁵⁴Mathesis, 1, 1881, 99-102. Nouv. Ann. Math., (3), 1, 1882, 240; 2, 1883, 239, 240. Also Cesàro,⁶¹ 113-123, 133.

$n = \infty$ of $T(n)/(n \log n)$ is 1; cf. (7); the mean of $\Sigma(d+p)^{-1}$ is $(1+1/2+\dots+1/p)/p$. As generalizations of Berger's⁵¹ results, the mean of $\Sigma d/p^d$ is $1/(p-1)$; the mean of the sum of the r th powers of the divisors of n is $n^r \zeta(r+1)$ and that of the inverses of their r th powers is $\zeta(r+1)$, where

$$(12) \quad \zeta(s) = \sum_{n=1}^{\infty} 1/n^s.$$

J. W. L. Glaisher⁵⁵ proved the last formula of Catalan⁴² and

$$\begin{aligned} \sigma(n) - \sigma(n-4) - \sigma(n-8) + \sigma(n-20) + \sigma(n-28) - \dots \\ = Q(n-1) + 3Q(n-3) - 6Q(n-6) - 10Q(n-10) + \dots, \end{aligned}$$

where $Q(n)$ is the number of partitions of n without repetitions, and 4, 8, 20, ... are the quadruples of the pentagonal numbers. He gave another formula of the latter type.

R. Lipschitz,⁵⁶ using his notations,⁵⁰ proved that

$$\begin{aligned} T(n) - \Sigma T \left[\frac{n}{a} \right] + \Sigma T \left[\frac{n}{ab} \right] - \dots = n + \Sigma \left[\frac{n}{P} \right], \\ G(n) - \Sigma aG \left[\frac{n}{a} \right] + \Sigma abG \left[\frac{n}{ab} \right] - \dots = n + \Sigma P \left[\frac{n}{P} \right], \\ D(n) - \Sigma D \left[\frac{n}{a} \right] + \Sigma D \left[\frac{n}{ab} \right] - \dots = \Phi(n) + \Sigma \Phi \left[\frac{n}{P} \right], \end{aligned}$$

where P ranges over those numbers $\leq n$ which are composed exclusively of primes other than given primes a, b, \dots , each $\leq n$.

Ch. Hermite⁵⁷ proved (11) very simply.

R. Lipschitz⁵⁸ considered the number $\tau_s(t)$ of those divisors of t which are exact s th powers of integers and proved that

$$\begin{aligned} \sum_{t=1}^n \tau_s(t) &= \sum_{j=1}^p \left[\frac{n}{j^s} \right] = \sum_{j=1}^n \left[\frac{n^{1/s}}{j^{1/s}} \right] \\ &= -\mu\nu + \sum_{x=1}^{\mu} \left[\frac{n}{x^s} \right] + \sum_{y=1}^{\mu} \left[\frac{n^{1/s}}{y^{1/s}} \right] = -\mu^2 + \sum_{x=1}^{\mu} \left[\frac{n}{x^s} \right] + \sum_{y=1}^{\mu} \left[\frac{n^{1/s}}{y^{1/s}} \right], \end{aligned}$$

where p^s is the largest s th power $\leq n$, and $\nu = [n/\mu^s]$. The last expression, found by taking $\mu = [n^{(1+s)^{-1}}]$, gives a generalization of (11).

T. J. Stieltjes⁵⁹ proved (7) by use of definite integrals.

E. Cesàro⁶⁰ proved (7) arithmetically and (11).

E. Cesàro⁶¹ proved that, if d ranges over the divisors of n , and δ over those of x ,

$$(13) \quad \Sigma G(d)f\left(\frac{n}{d}\right) = \Sigma g(d)F\left(\frac{n}{d}\right), \quad F(x) \equiv \Sigma f(\delta), \quad G(x) \equiv \Sigma g(\delta).$$

Taking $g(x) = 1$, $f(x) = x$, $\phi(x)$, $1/x$, we get the first two formulas of Liouville²⁵

⁵⁵Messenger Math., 12, 1882-3, 169-170.

⁵⁶Comptes Rendus Paris, 96, 1883, 327-9.

⁵⁷Acta Math., 2, 1883, 299-300.

⁵⁸Ibid., 301-4.

⁵⁹Comptes Rendus Paris, 96, 1883, 764-6.

⁶⁰Ibid., 1029.

⁶¹Mém. Soc. Sc. Liège, (2), 10, 1883, Mém. 6, pp. 26-34.

and the fourth of Liouville.²⁶ Taking $g=x$, $f=\phi$, we get the third formula of Liouville.²⁶ For $g=1/x$, $f=\phi$, we get

$$\sum d\phi(d)\sigma\left(\frac{n}{d}\right)=\sum d^2.$$

For $g=\phi$ or x^r , $f=x^s$, we get the first two of Liouville's²⁹ summation formulas.

If $\pi(x)$ is the product of the negatives of the prime factors $\neq 1$ of x ,

$$\sum \pi(d)\phi(d)\tau\left(\frac{n}{d}\right)\frac{1}{d^2}=\frac{\sigma(n)}{n}, \quad \sum \pi\left(\frac{n}{d}\right)\phi\left(\frac{n}{d}\right)\sigma(d)d^2=n\sum d^2,$$

$$\sum \pi(d)\phi(d)\sigma\left(\frac{n}{d}\right)\frac{1}{d}=\tau(n), \quad \sum \pi(d)\phi(d)\frac{1}{d^3}=\frac{1}{n^2}\sum d\phi(d).$$

Further specializations of (13) and of the generalization (p. 47)

$$\sum G(d)f\left(\frac{n}{d}\right)=\sum F(d)g\left(\frac{n}{d}\right), \quad F(x)\equiv\sum\psi(\delta)f\left(\frac{x}{\delta}\right), \quad G(x)\equiv\sum\psi(\delta)g\left(\frac{x}{\delta}\right),$$

led Cesàro (pp. 36-59) to various formulas of Liouville²⁵⁻²⁷ and many similar ones. It is shown (p. 64) that

$$\sum_{n=1}^{\infty} \frac{F(n)}{n^m} = \zeta(m) \sum_{n=1}^{\infty} \frac{f(n)}{n^m},$$

for ζ and F as in (12), (13). For $f(n)=\phi(n)$, we have the result quoted under Cesàro⁵⁷ in Ch. V. For $f(n)=1$ and n^k , $m-k>1$,

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^m} = \zeta^2(m), \quad \sum_n \frac{\sigma_k(n)}{n^m} = \zeta(m)\zeta(m-k).$$

If (n, j) is the g. c. d. of n, j , then (pp. 77-86)

$$\sum_{j=1}^n \frac{n}{(n, j)} = 2\sum\sigma(d) - 1, \quad n\tau(n) = \sum\sigma(n, j), \quad \sigma(n) = \sum\tau(n, j),$$

$$\sum_{j=1}^n \sigma_k(n, j) = n\sigma_{k-1}(n), \quad \sum j\sigma(n, j) = \frac{n}{2}\{n\tau(n) + \sigma(n)\}.$$

If in the second formula of Liouville²⁵ we take $m=1, \dots, n$ and add, we get

$$\sum_{j=1}^n \phi(j)T\left[\frac{n}{j}\right] = \sum_{j=1}^n \sigma(j).$$

Similarly (pp. 97-112) we may derive a relation in $[x]$ from any given relation involving all the divisors of x , or any set of numbers defined by x , such as the numbers a, b, \dots for which $x-a^2, x-b^2, \dots$ are all squares. Formula (7) is proved (pp. 124-8). It is shown (pp. 135-143) that the mean of the sum of the inverses of divisors of n which are multiples of k is $\pi^2/(6k^2)$; the excess of the number of divisors $4\mu+1$ over the number of divisors $4\mu+3$ is in mean $\pi/4$, and that for $4\mu+2$ and 4μ is $\frac{1}{2}\log 2$; the mean of the sum of the inverses of the odd divisors of any integer is $\pi^2/8$; the mean is found of various functions of the divisors. The mean (p. 172) of the number of divisors of an integer which are m th powers is $\zeta(m)$, and hence is $\pi^2/6$ if

$m=2$. The mean (pp. 216-9) of the number of divisors of the form $a\mu+r$ of n is, for $r>0$,

$$\frac{1}{r} + \frac{1}{a} \left\{ \log n/a + 2C - \int_0^1 \frac{1-x^{r/a}}{1-x} dx \right\}$$

(cf. pp. 341-2 and, for $a=4, 6$, pp. 136-8), while several proofs (also, p. 134) are given of the known result that the number of divisors of n which are multiples of a is in mean

$$\frac{1}{a} (\log n/a + 2C).$$

If (pp. 291-2) a ranges over the integers for which $[2n/d]$ is odd, the number (sum) of the a 's is the excess of the number (sum) of the divisors of $n+1, n+2, \dots, 2n$ over that of $1, \dots, n$; the means are $n \log 4$ and $\pi^2 n^2/6$. If (pp. 294-9) k ranges over the integers for which $[n/k]$ is odd, the number of the k 's is the excess of the number of odd divisors of $1, \dots, n$ over the number of their even divisors, and the sum of the k 's is the sum of the odd divisors of $1, \dots, n$; also

$$\Sigma \phi(k) = q^2, \quad q = \left[\frac{n+1}{2} \right].$$

Several asymptotic evaluations by Cesàro are erroneous. For instance, for the functions $\lambda(n)$ and $\mu(n)$, defined by Liouville²⁶ and Mertens,³⁷ Cesàro (p. 307, p. 157) gave as the mean values $6/\pi^2$ and $36/\pi^4$, whereas each is zero.⁶²

J. W. L. Glaisher⁶³ considered the sum $\Delta(n)$ of the odd divisors of n . If $n=2^r m$ (m odd), $\Delta(n) = \sigma(m)$. The following theorems were proved by use of series for elliptic functions:

$$\Delta(1)\Delta(2n-1) + \Delta(3)\Delta(2n-3) + \Delta(5)\Delta(2n-5) + \dots + \Delta(2n-1)\Delta(1)$$

equals the sum of the cubes of those divisors of n whose complementary divisors are odd. The sum of the cubes of all divisors of $2n+1$ is

$$\Delta(2n+1) + 12\{\Delta(1)\Delta(2n) + \Delta(2)\Delta(2n-1) + \dots + \Delta(2n)\Delta(1)\}.$$

If A, B, C are the sums of the cubes of those divisors of $2n$ which are respectively even, odd, with odd complementary divisor,

$$\begin{aligned} 2\Delta(2n) + 24\{\Delta(2)\Delta(2n-2) + \Delta(4)\Delta(2n-4) + \dots + \Delta(2n-2)\Delta(2)\} \\ = \frac{1}{3}(2A - 2B - C) = \frac{1}{7}(3 \cdot 2^{3r} - 10)B \end{aligned}$$

if $2n=2^r m$ (m odd). Halphen's formula⁴⁰ is stated on p. 220. Next,

$$\begin{aligned} n\sigma(2n+1) + (n-5)\sigma(2n-1) + (n-15)\sigma(2n-5) \\ + (n-30)\sigma(2n-11) + \dots = 0, \end{aligned}$$

⁶²H. v. Mangoldt, Sitzungsber. Ak. Wiss. Berlin, 1897, 849, 852; E. Landau, Sitzungsber. Ak. Wiss. Wien, 112, IIa, 1903, 537.

⁶³Quar. Jour. Math., 19, 1883, 216-223.

in which the differences between the arguments of σ in the successive terms are 2, 4, 6, 8, ..., and those between the coefficients are 5, 10, 15, ..., while $\sigma(0) = 0$. Finally, there is a similar recursion formula for $\Delta(n)$.

Glaisher⁶⁴ proved his⁴³ recursion formula for $\theta(n)$, gave a more complicated one and the following for $\sigma(n)$:

$$\sigma(n) - 2\{\sigma(n-1) + \sigma(n-2)\} + 3\{\sigma(n-3) + \sigma(n-4) + \sigma(n-5)\} - \dots \\ + (-1)^{r-1}r\{\dots + \sigma(1)\} = (-1)^s(s^3 - s)/6,$$

where $s = r$ unless $r\sigma(1)$ is the last term of a group, in which case, $s = r + 1$. He proved Jacobi's¹¹ statement and concluded from the same proof that $E(n) = \Pi E(n_i)$ if $n = \Pi n_i$, the n_i 's being relatively prime. It is evident that $E(p^r) = r + 1$ if p is a prime $4m + 1$, while $E(p^r) = 1$ or 0 if p is a prime $4m + 3$, according as r is even or odd. Also $E(2^r) = 1$. Hence we can at once evaluate $E(n)$. He gave a table of the values of $E(n)$, $n = 1, \dots, 1000$. By use of elliptic functions he found the recursion formulæ

$$E(n) - 2E(n-4) + 2E(n-16) - 2E(n-36) + \dots = 0 \text{ or } (-1)^{(\sqrt{n}-1)/2} \sqrt{n},$$

for n odd, according as n is not or is a square; for any n .

$$E(n) - E(n-1) - E(n-3) + E(n-6) + E(n-10) - \dots \\ = 0 \text{ or } (-1)^n \{(-1)^{(t-1)/2} t - 1\} / 4, \quad t \equiv \sqrt{8n+1},$$

according as n is not or is a triangular number 1, 3, 6, 10, He gave recursion formulæ for

$$S(2n) = E(2) + E(4) + \dots + E(2n), \\ S(2n-1) = E(1) + E(3) + \dots + E(2n-1).$$

The functions E , S , θ , σ are expressed as determinants.

J. P. Gram^{64a} deduced results of Berger⁵¹ and Cesàro.⁵⁴

Ch. Hermite⁶⁵ expressed $\sigma(1) + \sigma(3) + \dots + \sigma(2n-1)$, $\sigma(3) + \sigma(7) + \dots + \sigma(4n-1)$ and $\sigma(1) + \sigma(5) + \dots + \sigma(4n+1)$ as sums of functions

$$E_2(x) = \{[x]^2 + [x]\} / 2.$$

Chr. Zeller⁶⁶ gave the final formula of Catalan.⁴²

J. W. L. Glaisher⁶⁷ noted that, if in Halphen's⁴⁰ formula, n is a triangular number, $\sigma(n-n)$ is to be given the value $n/3$; if, however, we suppress the undefined term $\sigma(0)$, the formula is

$$\sigma(n) - 3\sigma(n-1) + 5\sigma(n-3) - \dots = 0 \text{ or } (-1)^{r-1}(1^2 + 2^2 + \dots + r^2),$$

according as n is not a triangular number or is the triangular number $r(r+1)/2$. He reproduced two of his^{63, 64, 76} own recursion formulas for $\sigma(n)$ (with ψ for σ in two) and added

$$\sigma(n) - \{\sigma(n-2) + \sigma(n-3) + \sigma(n-4)\} + \{\sigma(n-7) + \sigma(n-8) + \sigma(n-9) \\ + \sigma(n-10) + \sigma(n-11)\} - \{\sigma(n-15) + \dots\} + \dots = A - B,$$

⁶⁴Proc. London Math. Soc., 15, 1883-4, 104-122.

^{64a}Det K. Danske Vidensk. Selskabs Skrifter, (6), 2 1881-6 (1884), 215-220 296.

⁶⁵Amer. Jour. Math., 6, 1884, 173-4.

⁶⁶Acta Math., 4, 1884, 415-6.

⁶⁷Proc. Cambr. Phil. Soc., 5, 1884, 108-120.

where A and B denote the number of positive and negative terms respectively, not counting $\sigma(0) = n$ as a term;

$$\begin{aligned} & n\sigma(n) + 2\{(n-2)\sigma(n-2) + (n-4)\sigma(n-4)\} \\ & + 3\{(n-6)\sigma(n-6) + (n-8)\sigma(n-8) + (n-10)\sigma(n-10)\} + \dots \\ & = \sigma(n) + (1^2 + 3^2)\{\sigma(n-2) + \sigma(n-4)\} \\ & + (1^2 + 3^2 + 5^2)\{\sigma(n-6) + \sigma(n-8) + \sigma(n-10)\} + \dots \quad (n \text{ odd}). \end{aligned}$$

He reproduced his⁶⁴ formulas for $\theta(n)$ and $E(n)$. He announced (*ibid.*, p. 86) the completion of tables of the values of $\phi(n)$, $\tau(n)$, $\sigma(n)$ up to $n = 3000$, and inverse tables.

Möbius⁶⁸ obtained certain results on the reversion of series which were combined by J. W. L. Glaisher⁶⁹ into the general theorem: Let a, b, \dots be distinct primes; in terms of the undefined quantities e_a, e_b, \dots , let $e_n = e_a^{\alpha} e_b^{\beta} \dots$ if $n = a^{\alpha} b^{\beta} \dots$, and let $e_1 = 1$. Then, if

$$F(x) = \sum e_n f(x^n),$$

where n ranges over all products of powers of a, b, \dots , we have

$$f(x) = \sum (-1)^r e_{\nu} F(x^{\nu}),$$

where ν ranges over the numbers without square factors and divisible by no prime other than a, b, \dots , while r is the number of the prime factors of ν . Taking

$$e_n = n^r, \quad f(x) = \frac{x}{1-x},$$

Glaisher obtained the formula of H. J. S. Smith³⁸ and

$$\sigma_r(n) - \sum a^r \sigma_r\left(\frac{n}{a}\right) + \sum a^r b^r \sigma_r\left(\frac{n}{ab}\right) - \dots = 1.$$

Using the same f , but taking $e_2 = 0$, $e_p = p^r$, when p is an odd prime, he proved that, if $\Delta_r(n)$ is the sum of the r th powers of the odd divisors of n ,

$$\Delta_r(n) - \sum \Delta_r\left(\frac{n}{a}\right) + \sum \Delta_r\left(\frac{n}{ab}\right) - \dots = 0 \text{ or } n^r,$$

according as n is even or odd. In the latter case, it reduces to Smith's.

If $\Delta'_r(n)$ is the sum of the r th powers of those divisors of n whose complementary divisors are odd, while $E_r(n)$ [or $E'_r(n)$] is the excess of the sum of the r th powers of those divisors of n which [whose complementary divisors] are of the form $4m+1$ over the sum of the r th powers of those divisors which [whose complementary divisors] are of the form $4m+3$,

$$\Delta'_r(n) - \sum a^r \Delta'_r\left(\frac{n}{a}\right) + \sum a^r b^r \Delta'_r\left(\frac{n}{ab}\right) - \dots = \nu = \frac{1}{2}\{1 - (-1)^n\},$$

$$\Delta'_r(n) - \sum \Delta'_r\left(\frac{n}{A}\right) + \sum \Delta'_r\left(\frac{n}{AB}\right) - \dots = n^r,$$

⁶⁴Jour. für Math., 9, 1832, 105-123; Werke, 4, 591.

⁶⁸London, Ed. Dublin Phil. Mag., (5), 18, 1884, 518-540.

$$E_r(n) - \Sigma (-1)^{(A-1)/2} A^r E_r \left(\frac{n}{A} \right) + \Sigma (-1)^{(AB-1)/2} A^r B^r E_r \left(\frac{n}{AB} \right) - \dots = 1,$$

$$E_r(n) - \Sigma E_r \left(\frac{n}{a} \right) + \Sigma E_r \left(\frac{n}{ab} \right) - \dots = (-1)^{(n-1)/2} n^r \nu,$$

$$E'_r(n) - \Sigma a^r E'_r \left(\frac{n}{a} \right) + \Sigma a^r b^r E'_r \left(\frac{n}{ab} \right) - \dots = (-1)^{(n-1)/2} \nu,$$

$$E'_r(n) - \Sigma (-1)^{(A-1)/2} E'_r \left(\frac{n}{A} \right) + \Sigma (-1)^{(AB-1)/2} E'_r \left(\frac{n}{AB} \right) - \dots = n^r,$$

where A, B, \dots are the odd prime factors of n . Note that $\nu = 0$ or 1 according as n is even or odd. By means of these equations, each of the five functions $\sigma_r(n), \dots, E'_r(n)$ is expressed in two or more ways as a determinant of order n .

Ch. Hermite⁷⁰ quoted five formulas obtained by L. Kronecker⁷¹ from the expansions of elliptic functions and involving as coefficients the functions $\Phi(n) = \sigma(n)$, the sum $X(n)$ of the odd divisors of n , the excess $\Psi(n)$ of the sum of the divisors $> \sqrt{n}$ of n over the sum of those $< \sqrt{n}$, the excess $\Phi'(n)$ of the sum of the divisors of the form $8k \pm 1$ of n over the sum of the divisors of the form $8k \pm 3$, and the excess $\Psi'(n)$ of the sum of the divisors $8k \pm 1$ exceeding \sqrt{n} and the divisors $8k \pm 3$ less than \sqrt{n} over the sum of the divisors $8k \pm 1$ less than \sqrt{n} and the divisors $8k \pm 3$ exceeding \sqrt{n} . Hermite found the expansions into series of the right-hand members of the five formulas, employing the notations

$$\begin{aligned} E_1(x) &= [x + \tfrac{1}{2}] - [x], & E_2(x) &= [x][x+1]/2, \\ a &= 1, 3, 5, \dots; & b &= 2, 4, 6, \dots; & c &= 1, 2, 3, \dots, \end{aligned}$$

and A for a number of type a , etc. He obtained

$$X(1) + X(3) + \dots + X(A) = \Sigma E_2 \left(\frac{A+a}{2a} \right),$$

$$\sigma(1) + \sigma(2) + \dots + \sigma(C) = \Sigma E_2(C/c),$$

$$\Psi(1) + \Psi(2) + \dots + \Psi(C) = \Sigma E_2 \left(\frac{C-c^2}{c} \right),$$

$$X(2) + X(4) + \dots + X(B) = \tfrac{1}{3} \Sigma \left\{ a \left[\frac{B}{2a} \right] + b E_1 \left[\frac{B}{2b} \right] \right\},$$

$$\Phi'(1) + \Phi'(3) + \dots + \Phi'(A) = \Sigma (-1)^{(a^2-1)/8} a \left[\frac{A+a}{2a} \right],$$

$$\begin{aligned} \Psi'(1) + \Psi'(3) + \dots + \Psi'(A) &= \Sigma (-1)^{(a^2+7)/8} a \left\{ \left[\frac{A+2a-a^2}{2a} \right] \right. \\ &\quad \left. + \left[\frac{A-a^2}{2a} \right] - \left[\frac{A+a}{2a} \right] \right\}. \end{aligned}$$

⁷⁰Bull. Ac. Sc. St. Pétersbourg, 29, 1884, 340-3; Acta Math., 5, 1884-5, 315-9.

⁷¹Jour. für Math., 57, 1860, bottom p. 252 and top p. 253.

The first three had been found and proved purely arithmetically by Lipschitz and communicated to Hermite.

Hermite proved (11) by use of series. Also,

$$\sum_{a=1}^n F(a) = \sum_{a=1}^n \left[\frac{n}{a} \right] f(a), \quad F(n) \equiv \sum f(d),$$

where d ranges over the divisors of n . When $f(d) = 1$, $F(n)$ becomes $\tau(n)$ and the formula becomes the first one by Dirichlet.¹⁷

L. Gegenbauer⁷² considered the sum $\rho_{k,t}(n)$ of the k th powers of those divisors d_i of n whose complementary divisors are exact t th powers, as well as Jordan's function $J_k(n)$ [see Ch. V]. By means of the ζ -function, (12), he proved that

$$\sum_{m,n} \sigma_k(m) \rho_{0,2}(n) = \sum_d \rho_{0,2t}(d) \rho_{k,t} \left(\frac{r}{d} \right),$$

where d ranges over the divisors of r , and m, n over all pairs of integers for which $mn^t = r$;

$$\sum J_{ik}(n) \rho_{r,t}(m) = r^k \rho_{r-k,t}(r), \quad \sum \sigma_{r-k}(m) \tau(n) m^k = \sum \rho_{k,t}(d) \rho_{r,t} \left(\frac{r}{d} \right),$$

the latter for $t=1$ being Liouville's²⁹ seventh formula for $\nu=0$;

$$\sum d^r \rho_{k,t} \left(\frac{r}{d} \right) = \sum d^k \rho_{r,t} \left(\frac{r}{d} \right), \quad \sum J_r(d) d^k \rho_{k,t} \left(\frac{r}{d} \right) = \rho_{k+r,t}(r),$$

the latter for $t=\nu=1$, $k=0$, being the second formula of Liouville²⁵, while for $t=1$ it is the final formula by Cesàro²¹⁰ of Ch. V;

$$\sum \lambda(d) d^k \rho_{k,2t} \left(\frac{r}{d} \right) = \sum \lambda(d) \rho_{k,t}(d) \rho_{k,t} \left(\frac{r}{d} \right) = 0 \text{ or } \rho_{2k,t}(\sqrt{r}),$$

according as r is not or is a square;

$$\begin{aligned} \sum \lambda(n) \rho_{k,t}(m) &= \rho_{k,2t}(r), & \sum \lambda(d) \tau(d^2) &= \lambda(r) \tau(r), \\ \sum \tau^2(d) J_k \left(\frac{r}{d} \right) &= r^k \sum \frac{\tau(d^2)}{d^k}, & \sum d^k \tau(d^2) \sigma_k \left(\frac{r}{d} \right) &= \sum d^k \tau^2(d), \\ \sum_{x=1}^n \left[\frac{n}{x} \right] \tau(x^2) &= \sum_{r=1}^n \tau^2(r), & \sum_{x=1}^n \left[\frac{n}{x} \right] \lambda(x) \sigma_k(x) &= \sum_{r=1}^n \rho_{k,2}(r). \end{aligned}$$

By changing the sign of the first subscript of ρ , we obtain formulas for the sum $P_{k,t}(n) = n^k \rho_{-k,t}(n)$ of the k th powers of those divisors of n which are t th powers. By taking the second subscript of ρ to be unity, we get formulas for $\sigma_k(n)$. There are given many formulas involving also the number $f_a(n)$ of solutions of $n_1 n_2 \dots n_a = n$, and the number $\omega(n)$ of ways n can be expressed as a product of two relatively prime factors. Two special cases [(107), (128)] of these are the first formula of Liouville²⁶ and the ninth summation formula of Liouville,²⁹ a fact not observed by Gegenbauer. He proved that, if $p \leq n$,

$$\sum_{x=p+1}^n B(x) = - \sum_{x=A+1}^B C(x) + Bn - Ap,$$

⁷²Sitzungsber. Ak. Wiss. Wien (Math.), 89, II, 1884, 47-73, 76-79.

where

$$B(x) = \left[\sqrt[\tau]{\frac{bx^\sigma + \beta}{a}} - \rho \right], \quad C(x) = \left[\sqrt[\sigma]{\frac{a(x^\tau + \rho) - \beta}{b}} \right],$$

and $B = B(n)$, $A = B(p+1)$; also that

$$\sum_{x=p+1}^n D(x) = \sum_{x=D+1}^E F(x) + Dn - Ep,$$

where

$$D(x) = \left[\sqrt[\tau]{\frac{a}{bx^\sigma + \beta}} - \rho \right], \quad F(x) = \left[\sqrt[\sigma]{\frac{a}{b(x^\tau + \rho)} - \frac{\beta}{b}} \right],$$

and $D = D(n)$, $E = D(p+1)$. It is stated that special cases of these two formulas (here reported with greater compactness) were given by Dirichlet, Zeller, Berger and Cesàro. In the second, take $\tau = 1$, $\rho = 0$, and choose the integers a , β , b , n so that

$$bn^\sigma + \beta > a > b(n-1)^\sigma + \beta,$$

whence $D = 0$. If χ_r is the number of divisors of r which are of the form $bx^\sigma + \beta$, we get

$$\sum_{r=1}^a \chi_r = \sum_{x=1}^p \left[\frac{a}{bx^\sigma + \beta} \right] + \sum_{x=1}^E \left[\sqrt[\sigma]{\frac{a}{bx} - \frac{\beta}{b}} \right] - Ep, \quad E = \left[\frac{a}{b(p+1)^\sigma + \beta} \right].$$

Change n to $n+1$ and set $\beta = 0$, $b = \sigma = 1$, whence $a = n$ [also set $p = [\sqrt{n}]$]; we get Meissel's²² formula (11). Other specializations give the last one of the formulas by Lipschitz,⁵³ and

$$\sum_{r=1}^n k(r) = \sum_{x=1}^{\nu} \left[\frac{2n}{2x+1} \right] + \sum_{x=1}^{\nu} \left[\frac{n}{x} - \frac{1}{2} \right] - \nu^2 + t,$$

where $\nu = [\sqrt{n}]$, $k(r)$ is the number of odd divisors of r , while $t = 0$ or 1 according as $[n/\nu - \frac{1}{2}] > \nu - 1$ or $= \nu - 1$.

L. Gegenbauer⁷³ proved by use of ζ -functions many formulas involving his⁷² functions ρ , f and divisors d_i . Among the simplest formulas, special cases of the more general ones, are

$$\begin{aligned} \sum \sigma_k(d) d^\lambda &= \sum \sigma_{k+\lambda} \left(\frac{r}{d} \right) d^\lambda = \sum \sigma^\lambda \left(\frac{r}{d} \right) d^{k+\lambda}, & \sum \mu^2(d_4) &= \sum \lambda(h), \\ \sum \theta(h) \mu^2(d_2) &= \sum \mu^2(h), & \sum \tau(h^2) \mu^2(d_2) &= \sum \theta(h), & \sum \mu^2(d) \tau \left(\frac{r}{d} \right) &= \tau(r^2), \\ \sum \tau(d_2) \mu(h) &= \theta(r), & \sum \mu^2(d) J_k \left(\frac{r}{d} \right) &= \sum d_2^k \mu(h), \end{aligned}$$

summed for d , d_2 , d_4 , where $h = \sqrt{r/d_2}$. Other special cases are the fourth and sixth formulas of Liouville,²⁹ the first, third and last of Liouville.²⁵ Beginning with p. 414, the formulas involve also

$$\omega_k(n) = n^k \prod_{i=1}^r (1 + 1/p_i^k), \quad n = \prod_{i=1}^r p_i^{v_i}.$$

⁷³Sitzungsber. Ak. Wien (Math.), 90, II, 1884, 395-459. The functions used are not defined in the paper. For his ψ_n , ψ , ω , we write σ_n , τ , θ , where θ is the notation of Liouville.²⁵

Beginning with p. 425 and p. 430 there enter the two functions

$$n^\mu \prod_{i=1}^r \left(\frac{\Delta}{p_i} \right)^{\mu-1} \left\{ \left(\frac{\Delta}{p_i} \right) \mp p_i^{k-\mu} \right\},$$

in which (Δ/p) is Legendre's symbol, with the value 1 or -1 .

J. W. L. Glaisher⁷⁴ investigated the excess $\zeta_r(n)$ of the sum of the r th powers of the odd divisors of n over the sum of the r th powers of the even divisors, the sum $\Delta'_r(n)$ of the r th powers of those divisors of n whose complementary divisors are odd, wrote ζ for ζ_1 , and Δ' for Δ'_1 , and proved

$$\begin{aligned} \Delta'_3(n) &= n\Delta'(n) + 4\Delta'(1)\Delta'(n-1) + 4\Delta'(2)\Delta'(n-2) + \dots + 4\Delta'(n-1)\Delta'(1), \\ \zeta_3(n) &= (2n-1)\zeta(n) - 4\zeta(1)\zeta(n-1) - 4\zeta(2)\zeta(n-2) - \dots - 4\zeta(n-1)\zeta(1), \\ n\Delta'(n) &= \Delta'(1)\Delta'(2n-1) - \Delta'(2)\Delta'(2n-2) + \dots + \Delta'(2n-1)\Delta'(1), \\ (-1)^{n-1}n\zeta(n) &= \Delta'(n) + 8\zeta(1)\Delta'(n-2) + 8\zeta(2)\Delta'(n-4) + \dots, \\ \Delta'_3(n) &= n\Delta'(n) + \Delta'(2)\Delta'(2n-2) + \Delta'(4)\Delta'(2n-4) + \dots + \Delta'(2n-2)\Delta'(2), \\ -\zeta_3(n) &= 3\Delta(n) + 4\{\Delta(1)\Delta(n-1) + 9\Delta(2)\Delta(n-2) + \Delta(3)\Delta(n-3) \\ &\quad + 9\Delta(4)\Delta(n-4) + \dots + \Delta(n-1)\Delta(1)\} \quad (n \text{ even}), \\ \frac{2^{2r-1}\Delta'_{2r+1}(n)}{(2r)!} &= \frac{[1, 2r-1]}{1!(2r-1)!} + \frac{[3, 2r-3]}{3!(2r-3)!} + \dots + \frac{[2r-1, 1]}{(2r-1)!1!}, \end{aligned}$$

where

$$[p, q] = \sigma_p(1)\sigma_q(2n-1) + \sigma_p(3)\sigma_q(2n-3) + \dots + \sigma_p(2n-1)\sigma_q(1).$$

For n odd, $\zeta(n) = \Delta'(n) = \sigma(n)$ and the fourth formula gives

$$(n-1)\sigma(n) = 8\{\sigma(1)\sigma(n-2) + \zeta(2)\sigma(n-4) + \sigma(3)\sigma(n-6) + \zeta(4)\sigma(n-8) + \dots\}.$$

Glaisher⁷⁵ proved that

$$\begin{aligned} 5\sigma_3(n) - 6n\sigma(n) + \sigma(n) &= 12\{\sigma(1)\sigma(n-1) + \sigma(2)\sigma(n-2) + \dots + \sigma(n-1)\sigma(1)\}, \\ \sigma(1)\sigma(2n-1) + \sigma(3)\sigma(2n-3) + \dots + \sigma(2n-1)\sigma(1) &= \Delta'_3(n) = \frac{1}{8}\{\sigma_3(2n) - \sigma_3(n)\}. \end{aligned}$$

The latter includes the first theorem in his⁶³ earlier paper.

Glaisher⁷⁶ proved for Jacobi's¹¹ $E(n)$ that

$$\begin{aligned} \sigma(2m+1) &= E(1)E(4m+1) + E(5)E(4m-3) + E(9)E(4m-7) + \dots \\ &\quad + E(4m+1)E(1), \\ E(t) - 2E(t-4) + 2E(t-16) - 2E(t-36) + \dots &= 0 \quad (t=8n+5), \\ \sigma(v) - 2\sigma(v-4) + 2\sigma(v-16) - 2\sigma(v-36) + \dots &= 0 \quad (v=8n+7), \\ \sigma(u) + \sigma(u-8) + \sigma(u-24) + \sigma(u-48) + \dots &= 4\{\sigma(m) + 2\sigma(m-4) \\ &\quad + 2\sigma(m-16) + 2\sigma(m-36) + \dots\} \quad (m=2n+1, u=8n+3), \end{aligned}$$

and three formulas analogous to the last (pp. 125, 129). He repeated (p. 158) his⁷⁴ expressions for $\Delta'_3(n)$.

⁷⁴Messenger Math., 14, 1884-5, 102-8.

⁷⁵Ibid., 156-163.

⁷⁶Quar. Jour. Math., 20, 1885, 109, 116, 121, 118.

L. Gegenbauer⁷⁷ considered the number $\tau_1(k)$ of the divisors $\leq [\sqrt{n}]$ of k and the number $\tau_2(k)$ of the remaining divisors and proved that

$$\sum_{k=1}^n \tau_1(k) = \frac{n}{2}(\log_e n + 2C) + O(\sqrt{n}),$$

$$\sum \tau_2(k) = \frac{n}{2}(\log_e n + 2C - 2) + O(\sqrt{n}),$$

$O(s)$ being⁹⁰ of the order of magnitude of s . He proved (p. 55) that the mean of the sum of the reciprocals of the square divisors of any integer is $\pi^4/90$; that (p. 64) of the reciprocals of the odd divisors is $\pi^2/8$; the mean (p. 65) of the cubes of the reciprocals of the odd divisors of any integer is $\pi^4/96$, that of their fifth powers is $\pi^6/960$. The mean (p. 68) of Jacobi's¹¹ $E(n)$ is $\pi/4$.

G. L. Dirichlet⁷⁸ noted that in (7), p. 282 above, we may take ϵ to be of lower [unstated] order of magnitude than his former \sqrt{n} .

L. Gegenbauer⁷⁹ considered the sum $\tau_{r,k,s}(n)$ of the k th powers of those divisors of n which are r th powers and are divisible by no (sr) th power except 1; also the number $Q_a(b)$ of integers $\leq b$ which are divisible by no a th power except 1. It follows at once that, if $\mu_s(m) = 0$ if m is divisible by an s th power > 1 , but $= 1$ otherwise,

$$\tau_{r,k,s}(n) = \sum \mu_s \left(\sqrt[r]{\frac{n}{d_r}} \right) \frac{n^k}{d_r^k},$$

where the summation extends over all the divisors d_r of n whose complementary divisors are r th powers, and that

$$(14) \quad \sum_{x=1}^n \tau_{r,k,s}(x) = \sum_{x=1}^{\nu} \left[\frac{n}{x^r} \right] x^{rk} \mu_s(x), \quad \nu = [\sqrt[n]{n}].$$

From the known formula $Q_r(n) = \sum [n/x^r] \mu(x)$, $x = 1, \dots, \nu$, is deduced

$$\sum_{y=1}^{\nu} Q_r \left(\left[\frac{n}{y^r} \right] \right) y^k = \sum_{x=1}^{\nu} \left[\frac{n}{x^r} \right] \left\{ \sum \mu \left(\frac{x}{d} \right) d^k \right\},$$

the right member reducing to n for $k=0$ and thus giving a result due to Bougaief. From this special result and (14) is derived

$$\sum_{x=1}^n \tau_{r,0,s}(x) = \sum_{x=1}^{\nu} Q_{sr} \left(\left[\frac{n}{x^r} \right] \right).$$

From these results he derived various expressions for the mean value of $\tau_{r,-k,s}(x)$ and of the sum $\tau_{r,k,s}(n)$ of the k th powers of those divisors of n which are r th powers and are divisible by at least one (sr) th power other than 1. He obtained theorems of the type: The mean value of the number of square divisors not divisible by a biquadrate is $15/\pi^2$; the mean value of the excess of the number of divisors of one of the forms $4r\mu + j$ ($j = 1, 3, \dots, 2r-1$) over the number of the remaining odd divisors is

$$\frac{\pi}{4r} \sum_{l=1}^r \cot \frac{(2l-1)\pi}{4r}.$$

⁷⁷Denkschr. Akad. Wien (Math.), 49, I, 1885, 24.

⁷⁸Göttingen Nachrichten, 1885, 379; Werke, 2, 407; letter to Kronecker, July 23, 1858.

⁷⁹Sitzungsberichte Ak. Wiss. Wien (Math.), 91, II, 1885, 600-621.

L. Gegenbauer⁸⁰ considered the number $A_0(a)$ of those divisors of a which are congruent modulo k and have a complementary divisor $\equiv 1 \pmod{k}$. He proved that, if $\rho < k$,

$$\sum_{x=1}^{\sigma} A_0(kx - \rho) = \sum_{x=1}^{\sigma} \left[\frac{(k-1)x + \sigma - \rho}{kx - \rho} \right] = \sigma + \sum_{x=1}^a \left[\frac{\rho x + \sigma}{kx + 1} \right] \\ = \sigma + a + \sum_{x=1}^b \left[\frac{\sigma - 1 - (k - \rho)x}{kx + 1} \right], \quad a \equiv \left[\frac{\sigma - 1}{k - \rho} \right], \quad b \equiv \left[\frac{\sigma - 2}{2k - \rho} \right].$$

If we replace σ by $\sigma - 1$ and subtract, we obtain expressions for $A_0(k\sigma - \rho)$. The above formulas give, for $k=2$, $\rho=1$,

$$\sum_{x=1}^{\sigma} \tau(2x-1) = \sigma + \sum_{x=1}^{\sigma-1} \left[\frac{x+\sigma}{2x+1} \right], \quad \tau(2\sigma-1) = 2 + \sum_{x=1}^{\sigma-2} \left\{ \left[\frac{x+\sigma}{2x+1} \right] - \left[\frac{x+\sigma-1}{2x+1} \right] \right\},$$

and formulas of Bouniakowsky.³² The same developments show that an odd number a is a prime if

$$\left[\frac{a}{2(2x+1)} + \frac{1}{2} \right] = \left[\frac{a-2}{2(2x+1)} + \frac{1}{2} \right]$$

for $x \leq [(a-3)/2]$; likewise for $a=6k \pm 1$ if the same equality holds when $x \leq [(a-5)/6]$, with similar tests for $a=3n-1$, or $4n-1$.

C. Runge⁸¹ proved that $\tau(n)/n^\epsilon$ has the limit zero as n increases indefinitely, for every $\epsilon > 0$.

E. Catalan⁸² noted that, if x_{np} is the number of ways of decomposing a product of n distinct primes into p factors > 1 , order being immaterial, $x_{np} = px_{n-1,p} + x_{n-1,p-1} = \{ p^{n-1} - \binom{p-1}{1} (p-1)^{n-1} + \binom{p-1}{2} (p-2)^{n-1} - \dots \pm 1 \} \div \{(p-1)!\}$.

E. Cesàro⁸³ considered the number $F_m(x)$ of integers $\leq x$ which are not divisible by m th powers, and the number $T_m(x)$ of those divisors of x which are m th powers, evaluated sums involving these and other functions, and determined mean values and probabilities relating to the greatest square divisor of an arbitrary integer.

R. Lipschitz⁸⁴ considered the sum $k(m)$ of the odd divisors of m increased by half the sum of the even divisors, and the function $l(m)$ obtained by interchanging the words "even," "odd." He proved that

$$k(m) - 2k(m-1) + 2k(m-9) - \dots = (-1)^{m-1}m \text{ or } 0,$$

according as m is a square or is not;

$$l(m) + l(m-1) + l(m-3) + l(m-6) + \dots = -m \text{ or } 0,$$

according as m is a triangular number or is not;

$$K(m) = k(1) + k(2) + \dots + k(m) = [m] + \left[\frac{m}{2} \right] + 3 \left[\frac{m}{3} \right] + 2 \left[\frac{m}{4} \right] + \dots + \mu \left[\frac{m}{m} \right],$$

$$L(m) = l(1) + l(2) + \dots + l(m) = -[m] + 2 \left[\frac{m}{2} \right] - 3 \left[\frac{m}{3} \right] + 4 \left[\frac{m}{4} \right] - \dots,$$

⁸⁰Sitzungsberichte Ak. Wien. (Math.), 91, II, 1885, 1194-1201. ⁸¹Acta Math., 7, 1885, 181-3.

⁸²Mém. soc. roy. sc. Liège, (2), 12, 1885, 18-20; Mélanges Math., 1868, 18.

⁸³Annali di Mat., (2), 13, 1885, 251-268. Reprint "Excursions arith. à l'infini," 17-34.

⁸⁴Comptes Rendus Paris, 100, 1885, 845. Cf. Glaisher¹¹⁶, also Fergola²¹ of Ch. XI, Vol. II.

where $\mu = m$ or $m/2$ according as m is odd or even. Cf. Hacks.⁹⁶

M. A. Stern⁸⁵ noted that Zeller's⁸⁶ formula follows from $B = \rho A$, where

$$\frac{1}{p(x)} = A = \sum_{n=0}^{\infty} \psi(n)x^n, \quad \frac{\rho}{p(x)} = B = \sum_{n=1}^{\infty} \sigma(n)x^{n-1}, \quad \rho = 1 + 2x - 5x^4 - 7x^6 + \dots,$$

where $p(x)$ is defined by (1), $\psi(n)$ is the number of partitions of n , and the second equation follows from the equality of (3) and (4) after removing the factor x . Next, if $N(n)$ denotes the number of combinations of $1, 2, \dots, n$ without repetitions producing the sum n ,

$$\sum_{n=1}^{\infty} N(n)x^n = (1+x)(1+x^2)\dots = \frac{(1-x^2)(1-x^4)\dots}{(1-x)(1-x^2)\dots},$$

then by the second equation above,

$$\begin{aligned} B(1-x^2-x^4+x^{10}+x^{14}-\dots) &= \rho \sum N(n)x^n, \\ \sigma(n) - \sigma(n-2) - \sigma(n-4) + \sigma(n-10) + \sigma(n-14) - \dots \\ &= N(n-1) + 2N(n-2) - 5N(n-5) - 7N(n-7) + \dots, \end{aligned}$$

where $\sigma(n-n) = 0$, $N(n-n) = 1$.

S. Roberts⁸⁶ noted that Euler's⁸⁴ formula (2) is identical with Newton's relation $S_{-n} = S_{-n+1} + S_{-n+2} - \dots$ for obtaining the sum S_{-n} of the $(-n)$ th powers of the roots of $s=0$, where s and p are defined by (2). In p , the sum of the $(-n)$ th powers of the roots of $1-x^k=0$ is k or 0 according as k is or is not a divisor of n . Hence the like sum for p is $\sigma(n)$. [Cf. Waring⁹.] The process can be applied to products of factors $1-f(k)x^k$. His further results may be given the following simpler form. Let ϕ_n be the sum of the even divisors of n , and ψ_n the sum of the odd divisors, and set $s_n = \phi_n + 2\psi_n$ if n is even, $s_n = -2\psi_n$ if n is odd. By elliptic function expansions,

$$\begin{aligned} s_{2n} + 8\{s_{2n-1}\psi_1 + 3s_{2n-2}\psi_2 + s_{2n-3}\psi_3 + 3s_{2n-4}\psi_4 + \dots + s_1\psi_{2n-1}\} + 12n\psi_{2n} &= 0, \\ s_{2n+1} + 8\{s_{2n}\psi_1 + 3s_{2n-1}\psi_2 + \dots + 3s_1\psi_{2n}\} + (4n+2)\psi_{2n+1} &= 0, \end{aligned}$$

the coefficients being 1 and 3 alternately. He indicated a process for finding a recursion formula involving the sums of the cubes of the even divisors and the sums of the cubes of the odd divisors, but did not give the formula.

N. V. Bougaief^{86a} obtained, as special cases of a summation formula, $\sum_u \{8x + 5 - 5(2u-1)^2\} \sigma(2x+1-u^2+u) = 0$, $\sum \{n - 3\sigma(u)\} P\{n - \sigma(u)\} = 0$, where $P(n)$ is the number of solutions u, v of $\sigma(u) + \sigma(v) = n$.

L. Gegenbauer^{86b} proved that the number of odd divisors of $1, 2, \dots, n$ equals the sum of the greatest integers in $(n+1)/2, (n+2)/4, (n+3)/6, \dots, (2n)/(2n)$. The number of divisors of the form $Bx - \gamma$ of $1, \dots, n$ is expressed as a sum of greatest integers; etc.

J. W. L. Glaisher⁸⁷ considered the sum $\Delta_s(n)$ of the s th powers of the odd divisors of n , the like sum $D_s(n)$ for the even divisors, the sum $D'_s(n)$ of the

⁸⁵Acta Mathematica, 6, 1885, 327-8.

⁸⁶Quar. Jour. Math., 20, 1885, 370-8.

^{86a}Comptes Rendus Paris, 100, 1885, 1125, 1160.

^{86b}Denkschr. Akad. Wiss. Wien (Math.), 49, II, 1885, 111.

⁸⁷Messenger Math., 15, 1885-6, 1-20.

sth powers of the divisors of n whose complementary divisors are even, the excess $\zeta'_s(n)$ of the sum of the sth powers of the divisors whose complementary divisors are odd over that when they are even, and the similar functions⁷⁴ $\Delta'_s, \zeta_s, \sigma_s$. The seven functions can be expressed in terms of any two:

$$\begin{aligned}\Delta_s &= \sigma_s - 2^s D'_s, & D_s &= 2^s D'_s, & \Delta'_s &= \sigma_s - D'_s, \\ \zeta_s &= \sigma_s - 2^{s+1} D'_s, & \zeta'_s &= \sigma_s - 2D'_s,\end{aligned}$$

where the arguments are all n . Since $D'_s(2k) = \sigma_s(k)$, we may express all the functions in terms of $\sigma_s(n)$ and $\sigma_s(n/2)$, provided the latter be defined to be zero when n is odd. Employ the abbreviation $\Sigma fF = \Sigma Ff$ for

$$f(1)F(n-1) + f(2)F(n-2) + f(3)F(n-3) + \dots + f(n-1)F(1).$$

This sum is evaluated when f and F are any two of the above seven functions with $s=1$ (the subscript 1 is dropped). If

$$f(n) = a\sigma(n) + \beta D'(n), \quad F(n) = a'\sigma(n) + \beta' D'(n),$$

then

$$\Sigma fF = aa' \Sigma \sigma \sigma + (a\beta' + a'\beta) \Sigma \sigma D' + \beta\beta' \Sigma D' D'.$$

By using the first formula in each of two earlier papers,^{74, 75} we get

$$12 \Sigma \sigma \sigma = 5\sigma_3(n) - 6n\sigma(n) + \sigma(n),$$

$$12 \Sigma D' D' = 5D'_3(n) - 3nD'(n) + D'(n),$$

$$24 \Sigma \sigma D' = 2\sigma_3(n) + (1-3n)\sigma(n) + (1-6n)D'(n) + 8D'_3(n).$$

Hence all 21 functions can now be expressed at once linearly in terms of σ_3, D'_3, σ and D' . The resulting expressions are tabulated; they give the coefficients in the products of any two of the series $\Sigma_1^\infty f(n)x^n$, where f is any one of our seven functions without subscript.

Glaisher⁸⁸ gave the values of $\Sigma \sigma_3 \sigma_i$ for $i=3, 5, 9$ and $\Sigma \sigma_5 \sigma_7$, where the notation is that of the preceding paper. Also, if $\rho = n-r$,

$$12 \sum_{r=1}^n r \rho \sigma(r) \sigma(\rho) = n^2 \sigma_3(n) - n^3 \sigma(n), \quad \sum_{r=1}^n r f(r) F(\rho) = \frac{n}{2} \Sigma fF.$$

L. Gegenbauer⁸⁹ gave purely arithmetical proofs of generalizations of theorems obtained by Hermite⁷⁰ by use of elliptic function expansions. Let

$$S_k(r) = \sum_{j=1}^r j^k, \quad \sigma = \sum_{x=1}^r S_k \left(\left[\frac{n}{x} \right] \right) - \nu S_k(\nu), \quad \nu \equiv [\sqrt{n}].$$

Then (p. 1059),

$$\sum_{x=1}^n \left[\frac{n}{x} \right] x^k = \sum_{x=1}^r \left[\frac{n}{x} \right] x^k + \sigma.$$

The left member is known to equal the sum of the k th powers of all the divisors of $1, 2, \dots, n$. The first sum on the right is the sum of the k th powers of the divisors $\leq \sqrt{n}$ of $1, \dots, n$. Hence if $\Lambda_k(x)$ is the excess of the

⁸⁸Messenger Math., 15, 1885-6, p. 36.

⁸⁹Sitzungsberichte Ak. Wien (Math.), 92, II, 1886, 1055-78.

sum $\psi'_k(x)$ of the k th powers of the divisors $> \sqrt{x}$ of x over the sum of the k th powers of the remaining divisors, it follows at once that

$$\sum_{x=1}^n \Lambda_k(x) = - \sum_{x=1}^{\nu} \left[\frac{n}{x} \right] x^k + \sigma.$$

Also

$$\sum_{x=1}^n \psi'_k(x) = \sum_{x=1}^{\nu} S_k \left(\left[\frac{n}{x} \right] \right) + S_{k+1}(\nu) - (\nu+1)S_k(\nu),$$

with a similar formula for $\Sigma \Psi_k(x)$, where $\Psi_k(x)$ is the excess of $\psi'_k(x)$ over the sum of the k th powers of the divisors $< \sqrt{x}$ of x . For $k=1$, the last formula reduces to the third one of Hermite's.

Let $\chi_k(x)$ be the sum of the k th powers of the odd divisors of x ; $\chi_k''(x)$ that for the odd divisors $> \sqrt{x}$; $X_k''(x)$ the excess of the latter sum over the sum of the k th powers of the odd divisors $< \sqrt{x}$ of x ; $\chi_k'''(x)$ the excess of the sum of the k th powers of the divisors $8s \pm 1 > \sqrt{x}$ of x over the sum of the k th powers of the divisors $8s \pm 3 < \sqrt{x}$ of x . For $y=2x$ and $y=2x-1$, the sum from $x=1$ to $x=n$ of $\chi_k(y)$, $\chi_k''(y)$, $X_k''(y)$ and $\chi_k'''(y)$ are expressed as complicated sums involving the functions S_k and $[x]$.

E. Pfeiffer⁹⁰ attempted to prove a formula like (7) of Dirichlet,¹⁷ where now ϵ is $O(n^{1/3+k})$ for every $k > 0$. Here $Og(T)$ means a function whose quotient by $g(T)$ remains numerically less than a fixed finite value for all sufficiently large values of T . E. Landau⁹¹ noted that the final step in the proof fails from lack of uniform convergence and reconstructed the proof to secure this convergence.

L. Gegenbauer,⁹² in continuation of his⁸⁰ paper, gave similar but longer expressions for

$$\sum_{x=0}^{\sigma} \tau(y), \quad \sum_{x=0}^{\sigma} \sigma_k(y) \quad (y=4x+1, 6x+1, 8x+3, 8x+5, 8x+7)$$

and deduced similar tests for the primality of y .

Gegenbauer^{92a} found the mean of the number of divisors $\lambda x + a$ of a number of s digits with a complementary divisor $\mu y + \beta$; also for divisors $ax^2 + by^2$.

Gegenbauer^{92b} evaluated $A(1) + \dots + A(n)$ where $A(x)$ is the sum of the p th powers of the σ th roots of those divisors d of x which are exact σ th powers and whose complementary divisors exceed $kd^{r/\sigma}$. A special case gives (11), p. 284 above.

Gegenbauer^{92c} gave a formula involving the sum of the k th powers of those divisors of $1, \dots, m$ whose complementary divisors are divisible by no r th power > 1 .

⁹⁰Ueber die Periodicität in der Teilbarkeit. . . , Jahresbericht der Pfeiffer'schen Lehr- und Erziehungs-Anstalt zu Jena, 1885-6, 1-21.

⁹¹Sitzungsber. Ak. Wiss. Wien (Math.), 121, IIa, 1912, 2195-2332; 124, IIa, 1915, 469-550. Landau.¹⁶¹

⁹²*Ibid.*, 93, II, 1886, 447-454.

^{92a}Sitzungsber. Ak. Wiss. Wien (Math.), 93, 1886, II, 90-105.

^{92b}*Ibid.*, 94, 1886, II, 35-40.

^{92c}*Ibid.*, 757-762.

Ch. Hermite⁹³ proved that if $F(N)$ is the number of odd divisors of N ,

$$\sum_{n=1}^{\infty} q^{(n^2+n)/2} / (1-q^n) = \Sigma F(N) q^N,$$

and then that

$$F(1) + F(2) + \dots + F(N) = \frac{1}{2} N \log N + \left(C - \frac{1}{4}\right) N,$$

$$\Phi(1) + \Phi(2) + \dots + \Phi(N) = \frac{1}{2} N \log N/k + \left(C - \frac{1}{2}\right) N,$$

asymptotically, where $\Phi(N)$ is the number of decompositions of N into two factors d, d' , such that $d' > kd$.

E. Catalan^{93a} noted that, if $n = i + i' = 2i''d$,

$$\Sigma \sigma(i) \sigma(i') = \Sigma d^3, \quad \Sigma \{ \sigma(i) \sigma(2n-i) \} = 8 \Sigma \{ \sigma(i) \sigma(n-i) \}.$$

E. Cesàro⁹⁴ proved Lambert's⁷ result that $\tau(n)$ is the coefficient of x^n in $\Sigma x^k / (1-x^k)$. Let $T_\nu(n)$ be the number of sets of positive integral solutions of

$$\xi_1 + 2\xi_2 + \dots + \nu\xi_\nu = n$$

and $s_\nu(n)$ the sum of the values taken by ξ_ν . Then

$$s_\nu(n) = T_\nu(n) + T_\nu(n-\nu) + T_\nu(n-2\nu) + \dots,$$

$$\tau(n) = s_1(n) - s_2(n) + s_3(n) - \dots$$

Let

$$t_n(x) = \Sigma (-1)^{d+1} T_d(x-n),$$

summed for the divisors d of n . Then

$$\tau(n) = t_1(n) + t_2(n) + \dots + T_1(n) - T_2(n) + T_3(n) - \dots$$

E. Busche⁹⁵ employed two complementary divisors δ_m and δ'_m of m , an arbitrary function f , and a function $y = \Phi(x)$ increasing with x whose inverse function is $x = y\psi(y)$. Then

$$\sum_{x=1}^a \{ f([\psi(x)], x) - f(0, x) \} = \Sigma \{ f(\delta'_m, \delta_m) - f(\delta'_m - 1, \delta_m) \},$$

where in the second member the summation extends over all divisors of all positive integers, and $\Phi(m) \leq \delta_m \leq a$. In particular,

$$\sum_{x=1}^a f(x) [\psi(x)] = \Sigma f(\delta_m), \quad \sum_{x=1}^a [\psi(x)] = \text{number of } \delta_m,$$

subject to the same inequalities. In the last equation take $\psi(x) = x$, $a = [\sqrt{n}]$; we get (11).

J. Hacks⁹⁶ proved that, if m is odd,

$$\mathfrak{F}(m) \equiv \tau(1) + \tau(3) + \tau(5) + \dots + \tau(m) = \Sigma \left[\frac{m+t}{2t} \right],$$

⁹³Jour. für Math., 99, 1886, 324-8.

^{93a}Mém. Soc. R. Sc. Liège, (2), 13, 1886, 318 (Mélanges Math., II).

⁹⁴Jornal de sciencias math. e astr., 7, 1886, 3-6.

⁹⁵Jour. für Math., 100, 1887, 459-464. Cf. Busche.¹⁰³

⁹⁶Acta Math., 9, 1887, 177-181. Corrections, Hacks,⁹⁷ p. 6, footnote.

$$\mathfrak{G}(m) \equiv \sigma(1) + \sigma(3) + \sigma(5) + \dots + \sigma(m) = \sum t \left[\frac{m+t}{2t} \right],$$

where t ranges over the odd integers $\leq m$. For the K and L of Lipschitz⁸⁴ and $G(m) = \sigma(1) + \sigma(2) + \dots + \sigma(m)$, it is shown that

$$\mathfrak{F}(m) \equiv \mathfrak{G}(m) \equiv \left[\frac{\sqrt{m+1}}{2} \right] \equiv K(m) \pmod{2},$$

$$L(m) \equiv G(m) \equiv [\sqrt{m}] + \left[\sqrt{\frac{m}{2}} \right], \quad T(m) \equiv [\sqrt{m}] \pmod{2}.$$

J. Hacks⁹⁷ gave a geometrical proof of (11) and of Dirichlet's¹⁷ expression for $T(n)$, just preceding (7). He proved that the sum of all the divisors, which are exact ath powers, of $1, 2, \dots, m$ is

$$\sum_{j=1}^m \{1^a + 2^a + \dots + [\sqrt{a/m/j}]^a\}.$$

He gave (pp. 13-15) several expressions for his⁹⁶ $\mathfrak{F}(m)$, $\mathfrak{G}(m)$, $K(m)$.

L. Gegenbauer^{97a} gave simple proofs of the congruences of Hacks.⁹⁶

M. Lerch⁹⁸ considered the number $\psi(a, b)$ of divisors $> b$ of a and proved that

$$(15) \quad \sum_{\rho=0}^{[n/2]} \psi(n-\rho, \rho) = n, \quad \sum_{\rho=0}^n \psi(n+\rho, \rho) = 2n.$$

A. Strnad⁹⁹ considered the same formulas (15).

M. Lerch¹⁰⁰ considered the number $\chi(a, b)$ of the divisors $\leq b$ of a and proved that

$$\begin{aligned} \sum_{\sigma=0}^{[(m-1)/a]} \{ \psi(m-\sigma a, k+\sigma) - \chi(m-\sigma a, a) \} \\ + \sum_{\lambda=1}^k \{ \psi(m+\lambda a, \lambda-1) - \chi(m+\lambda a, a) \} = 0. \end{aligned}$$

This reduces to his (15) for $a=1$, $k=1$ or $m+1$. Let $(k, n; m)$ denote the g. c. d. (k, n) of k, n or zero, according as (k, n) is or is not a divisor of m . Then

$$(16) \quad \sum_{a=0}^{a-1} \{ \psi(m+an, a) - \psi(m+an, a) \} = \sum_{k=1}^a (k, n; m).$$

In case m and n are relatively prime, the right member equals the number $\phi(a, n)$ of integers $\leq a$ which are prime to n . Finally, it is stated that

$$(17) \quad \sum_{a=0}^c \psi(m-an, a) = \sum_{a=0}^c \chi(m-an, n), \quad c = \left[\frac{m-1}{n} \right].$$

Gegenbauer,²⁹ Ch. VIII, proved (16) and the formula preceding it.

⁹⁷Acta Math., 10, 1887, 9-11.

^{97a}Sitzungsber. Ak. Wiss. Wien (Math.), 95, 1887, II, 297-8.

⁹⁸Prag Sitzungsberichte (Math.), 1887, 683-8.

⁹⁹Casopis mat. fys., 18, 1888, 204.

¹⁰⁰Compt. Rend. Paris, 106, 1888, 186. Bull. des sc. math. et astr., (2), 12, I, 1888, 100-108, 121-6.

C. A. Laisant¹⁰¹ considered the number $n_k(N)$ of ways N can be expressed as a product of k factors (including factors unity), counting $PQ \dots$ and $QP \dots$ as distinct decompositions. Then

$$n_k(N) = n_{k-1}(N) \Pi \left(1 + \frac{e_i}{k-1} \right), \quad N = \Pi p_i^{e_i}.$$

E. Cesàro¹⁰² proved Gauss' result that the number of divisors, not squares, of n is asymptotic to $6\pi^{-2} \log n$. Hence $\tau(n^2)$ is asymptotic to $3\pi^{-2} \log^2 n$. The number of decompositions of n into two factors whose g. c. d. has a certain property is asymptotic to the product of $\log n$ by the probability that the g. c. d. of two numbers taken at random has the same property.

E. Busche¹⁰³ gave a geometric proof of his⁹⁵ formula. But if we take $\Phi(x)$ to be a continuous function decreasing as x increases, with $\Phi(0) > 0$, then the number of positive divisors of y which are $\leq \psi(y)$ is $\Sigma [\Phi(x)/x]$, summed for $x = 1, 2, \dots$, with $\Phi(x) \geq 0$. This result is extended to give the number of non-associated divisors of $y + zi$ whose absolute value is $\leq \phi(y, z)$.

J. W. L. Glaisher¹⁰⁴ considered the excess $H(n)$ of the number of divisors $\equiv 1 \pmod{3}$ of n over the number of divisors $\equiv 2 \pmod{3}$, proved that $H(pq) = H(p)H(q)$ if p, q are relatively prime, and discussed the relation of $H(n)$ to Jacobi's¹¹ $E(n)$.

Glaisher¹⁰⁵ gave recursion formulae for $H(n)$ and a table of its values for $n = 1, \dots, 100$.

L. Gegenbauer¹⁰⁶ found the mean value of the number of divisors of an integer which are relatively prime to given primes p_1, \dots, p_s , and are also $(\rho\tau)$ th powers and have a complementary divisor which is divisible by no τ th powers. Also the mean of the sum of the reciprocals of the k th powers of those divisors of an integer which are prime to p_1, \dots, p_s and are r th powers. Also many similar theorems.

Gegenbauer^{106a} expressed $\sum_{x=0}^{x=n} F(4x+1)$ and $\Sigma F(4x+3)$ in terms of Jacobi's symbols (Δ/y) and greatest integers $[y]$ when $F(x)$ is the sum of the k th powers of those divisors $\leq \sqrt{x}$ of x which are prime to D , or are divisible by no r th power > 1 , etc.; and gave asymptotic evaluations of these sums.

J. P. Gram¹⁰⁷ considered the number $D_n(m)$ of divisors $\leq m$ of n , the number $N_{2,3,\dots}(n)$ of integers $\leq n$ which are products of powers of the primes 2, 3, ..., and the sum $L_{2,3,\dots}(n)$ of the values of $\lambda(k)$ whose arguments k are the preceding N numbers, where $\lambda(2^\alpha 3^\beta \dots) = (-1)^{\alpha+\beta+\dots}$.

If $p = p_1^{a_1} p_2^{a_2} \dots$, where the p_i are distinct primes,

$$D_p(n) = N(n) - \Sigma N(n/p_1^{a_1+1}) + \Sigma N(n/p_1^{a_1+1} p_2^{a_2+1}) - \dots$$

¹⁰¹Bull. Soc. Math. France, 16, 1888, 150.

¹⁰²Atti R. Accad. Lincei, Rendiconti, 4, 1888, I, 452-7.

¹⁰³Jour. für Math., 104, 1889, 32-37.

¹⁰⁴Proc. London Math. Soc., 21, 1889-90, 198-201, 209.

¹⁰⁵*Ibid.*, 395-402. See Glaisher.¹⁴¹

¹⁰⁶Denkschriften Ak. Wiss. Wien (Math.), 57, 1890, 497-530.

^{106a}Sitzungsber. Ak. Wiss. Wien (Math.), 99, 1890, IIa, 390-9.

¹⁰⁷Det K. Danske Videnskab. Selskabs Skrifter (natur. og math.), (6), 7, 1890, 1-28, with résumé in French, 29-34.

In particular, if the p_i include all the primes in order, we may replace $N(x)$ by $[x]$, the greatest integer $\leq x$. Since there are as many divisors $> a$ of n as there are divisors $< n/a$,

$$D_p(n) + D_p\left(\frac{p}{n}\right) = \epsilon + \Pi(a_i + 1),$$

where $\epsilon = 1$ or 0 according as n is or is not a divisor of p . These two formulas serve as recursion formulas for the computation of $N(n)$. For the case of two primes $p_1 = 2$, $p_2 = 3$,

$$N(2^x) = x + 1 + \sum_{j=1}^x \left[\frac{j \log 2}{\log 3} \right], \quad N(3^y) = y + 1 + \sum_{j=1}^y \left[\frac{j \log 3}{\log 2} \right].$$

The functions L satisfy similar formulas and are computed similarly.

J. W. L. Glaisher¹⁰⁸ stated a theorem, which reduces for $m=1$ to Halphen's,⁴⁰

$$S \equiv \sigma_m(n) - 3\sigma_m(n-1) + 5\sigma_m(n-3) - 7\sigma_m(n-6) + 9\sigma_m(n-10) - \dots$$

$$= 2 \sum_k \binom{m}{k} \{ \sigma_{m-k}(n-1) - (1^k + 2^k) \sigma_{m-k}(n-3) + (1^k + 2^k + 3^k) \sigma_{m-k}(n-6) - \dots \} \\ + \delta(-1)^{g-1} (1 + 2^{m+1} + 3^{m+1} + \dots + g^{m+1}),$$

provided m is odd, where k ranges over the even numbers $2, 4, \dots, m-1$, while $\delta = 0$ or $\delta = 1$ according as n is not or is of the form $g(g+1)/2$. As in Glaisher⁶⁷ for $m=1$, the series are stopped before any term $\sigma_i(n-n)$ is reached; but, if we retain such terms, we must set $\delta = 0$ for every n and define $\sigma_i(0)$ by

$$\sigma(0) = \frac{n}{m+2}, \quad \binom{m}{3} \sigma_3(0) = \left\{ \frac{m}{m+2} - (m+1) B_1 \right\} n, \\ \binom{m}{5} \sigma_5(0) = \left\{ \frac{m}{m+2} - (m+1) B_1 + \binom{m+1}{3} \frac{B_2}{2} \right\} n, \\ \binom{m}{7} \sigma_7(0) = \left\{ \frac{m}{m+2} - (m+1) B_1 + \binom{m+1}{3} \frac{B_2}{2} - \binom{m+1}{5} \frac{B_3}{3} \right\} n, \dots,$$

where B_1, B_2, \dots are the Bernoullian numbers.

Glaisher¹⁰⁹ stated the simpler generalization of Halphen⁴⁰:

$$S + \sum_k \frac{1}{2^k(k+1)} \binom{m}{k} \{ \sigma_{m-k}(n) - 3^{k+1} \sigma_{m-k}(n-1) + 5^{k+1} \sigma_{m-k}(n-3) - \dots \} \\ = \delta(-1)^{g-1} \frac{1}{2^{m+1}(m+1)} \{ g(2g+1)^{m+1} - 1 - 3^{m+1} - 5^{m+1} - \dots - (2g-1)^{m+1} \},$$

where the summation index k ranges over the even numbers $2, 4, \dots, m-1$, and m is odd. If we include the terms $\sigma_{2r-1}(0) = (-1)^r B_r / (4r)$ in the left member, the right member is to be replaced by

$$\delta(-1)^{g-1} \frac{(2g+1)^{m+2}}{2^{m+2}(m+2)}.$$

¹⁰⁸Messenger Math., 20, 1890-1, 129-135.

¹⁰⁹Ibid., 177-181.

Glaisher¹¹⁰ considered the set $G_n\{\psi(d), \chi(d), \dots\}$ of the values of $\psi(d), \chi(d), \dots$ when d ranges over all the divisors of n , and wrote $-G(\psi, \chi, \dots)$ for $G(-\psi, -\chi, \dots)$. By use of the ζ -function (12), he proved (p. 377) that the numbers given by

$$G_n(d) - G_{n-1}(d, d \neq 1) + G_{n-3}(d, d \neq 1, d \neq 2) - G_{n-6}(d, d \neq 1, d \neq 2, d \neq 3) + \dots$$

all cancel if n is not a triangular number, but reduce to one 1, two 2's, three 3's, ..., g g 's, each taken with the sign $(-)^{g-1}$, if n is the g th triangular number $g(g+1)/2$. For example, if $n=6$, whence $g=3$,

$$\begin{aligned} \{1, 2, 3, 6\} - \{1, 5; 2, 6; 0, 4\} + \{1, 3; 2, 4; 0, 2; 3, 5; -1, 1\} \\ = \{1, 2, 2, 3, 3, 3\}. \end{aligned}$$

Let $\psi(d)$ be an odd function, so that $\psi(-d) \equiv -\psi(d)$, and let $\Sigma_r f(d)$ denote the sum of the values of $f(d)$ when d ranges over the divisors of r . Then the above theorem implies that

$$\begin{aligned} \Sigma_n \psi(d) - \Sigma_{n-1} \{\psi(d) + \psi(d \neq 1)\} + \Sigma_{n-1-2} \{\psi(d) + \psi(d \neq 1) + \psi(d \neq 2)\} \\ - \Sigma_{n-1-2-3} \{\psi(d) + \psi(d \neq 1) + \psi(d \neq 2) + \psi(d \neq 3)\} + \dots \\ = \delta(-1)^{g-1} \{\psi(1) + 2\psi(2) + 3\psi(3) + \dots + g\psi(g)\}, \end{aligned}$$

where $\delta=0$ or 1 according as n is not or is of the form $g(g+1)/2$, and where $\psi(d \neq i)$ is to be replaced by $\psi(d+i) + \psi(d-i)$. Taking $\psi(d) = d^m$, where m is odd, we obtain Glaisher's¹⁰⁸ recursion formula for $\sigma_m(n)$, other forms of which are derived. For the function⁷⁴ ζ_3 , we derive

$$\begin{aligned} \zeta_3(n) + \zeta_3(n-1) + \zeta_3(n-3) + \dots + 6\{\zeta(n-1) - (1^2-2^2)\zeta(n-3) \\ + (1^2-2^2+3^2)\zeta(n-6) - \dots\} \\ = (-1)^{g-1}(1^4-2^4+3^4-\dots+(-1)^{g-1}g^4) \text{ or } 0, \end{aligned}$$

according as n is of the form $g(g+1)/2$ or not.

Next he proved a companion theorem to the first:

$$G_n\left(\begin{matrix} 2d+1 \\ -[2d-1] \end{matrix}\right) - G_{n-1}\left(\begin{matrix} 2d+3 \\ -[2d-3] \end{matrix}\right) + G_{n-3}\left(\begin{matrix} 2d+5 \\ -[2d-5] \end{matrix}\right) - G_{n-6}\left(\begin{matrix} 2d+7 \\ -[2d-7] \end{matrix}\right) + \dots$$

all cancel if n is not a triangular number, but reduce to 1, 3, 5, ..., $2g-1$, each taken with the sign $(-)^g$, together with $(-1)^{g+1}(2g+1)$ taken g times, if n is the g th triangular number $g(g+1)/2$. For example, if $n=6$,

$$\begin{aligned} \left\{ \begin{matrix} 3, & 5, & 7, & 13 \\ -1, & -3, & -5, & -11 \end{matrix} \right\} - \left\{ \begin{matrix} 5, & 13 \\ -1, & -7 \end{matrix} \right\} + \left\{ \begin{matrix} 7, & 11 \\ -3, & -1 \end{matrix} \right\} = \left\{ -1, -3, -5, 7, 7, 7 \right\}. \end{aligned}$$

Hence if $\chi(d)$ be any even function, so that $\chi(-d) = \chi(d)$,

$$\begin{aligned} \Sigma_n \{\chi(2d+1) - \chi(2d-1)\} - \Sigma_{n-1} \{\chi(2d+3) - \chi(2d-3)\} + \Sigma_{n-3} - \dots \\ = \delta(-1)^{g-1} \{g\chi(2g+1) - \chi(1) - \chi(3) - \dots - \chi(2g-1)\}. \end{aligned}$$

Taking $\chi(k) = k^{m+1}$, where k and m are odd, we get Glaisher's¹⁰⁹ formula.

¹¹⁰Proc. London Math. Soc., 22, 1890-1, 359-410. Results stated in London, Edinb., Dublin Phil. Mag., (5), 33, 1892, 54-61.

He proved two theorems relating to the divisors of $1, 2, \dots, n$:

$$G_n \left(\begin{matrix} d+1 \\ -[d-1] \end{matrix} \right) - (G_{n-1} + G_{n-2}) \left(\begin{matrix} -d+2 \\ -[d-2] \end{matrix} \right) \\ + (G_{n-3} + G_{n-4} + G_{n-5}) \left(\begin{matrix} d+3 \\ -[d-3] \end{matrix} \right) - \dots$$

all cancel with the exception of $-2, -4, \dots, -(p-2)$, each taken twice, p taken $p-1$ times and -0 , if p be even; but with the exception of $1, 3, \dots, p-2$, each taken twice, and $-p$ taken $p-1$ times, if p be odd, where $p(p+1)/2$ is the triangular number next $>n$;

$$G_n(d) - (G_{n-1} + G_{n-2})(d \pm 1) + (G_{n-3} + G_{n-4} + G_{n-5})(d, d \pm 2) \\ - (G_{n-6} + \dots + G_{n-9})(d \pm 1, d \pm 3) + (G_{n-10} + \dots + G_{n-14})(d, d \pm 2, d \pm 4) - \dots$$

all cancel with the exception of k taken k times, for $k=1, 3, 5, \dots, p-1$, if p be even; and of $-k$ taken k times, for $k=2, 4, 6, \dots, p-1$, if p be odd; here zeros are ignored.

The last two theorems yield (as before) corresponding relations for any even function χ and any odd function ψ . Applying them to $\chi(d+1) = (d+1)^m$ and $\psi(d) = d^m$, where m is odd, and in the first case dividing by $2(m+1)$, and modifying the right members, we get for

$$T \equiv \sigma_m(n) - 2\{\sigma_m(n-1) + \sigma_m(n-2)\} + 3\{\sigma_m(n-3) \\ + \sigma_m(n-4) + \sigma_m(n-5)\} - \dots$$

the respective relations

$$T + \sum_k \frac{1}{k+1} \binom{m}{k} \{\sigma_{m-k}(n) - 2^{k+1}(\sigma_{m-k}(n-1) + \sigma_{m-k}(n-2)) \\ + 3^{k+1}(\text{next three}) - \dots\} \\ = (-1)^p \left\{ \frac{p^{m+2}}{2(m+2)} - B_1 p^m + \frac{2^2}{3} \binom{m}{2} \frac{B_2}{2} p^{m-2} - \frac{2^4}{5} \binom{m}{4} \frac{B_3}{3} p^{m-4} + \dots \pm 2^{m-1} \frac{B_s}{s} p \right\},$$

where $s = (m+1)/2$ and $\sigma_i(0)$ terms are suppressed;

$$T = \sum_k 2 \binom{m}{k} \{\sigma_{m-k}(n-1) + \sigma_{m-k}(n-2) - 2^k(\text{next three}) + (1^k + 3^k)(\text{next four}) \\ - (2^k + 4^k)(\text{next five}) + (1^k + 3^k + 5^k)(\text{next six}) - (2^k + 4^k + 6^k)(\text{next seven}) + \dots\} \\ + \begin{cases} 1^{m+1} + 3^{m+1} + 5^{m+1} + \dots + (p-1)^{m+1}, & \text{if } p \text{ be even,} \\ -2^{m+1} - 4^{m+1} - 6^{m+1} - \dots - (p-1)^{m+1}, & \text{if } p \text{ be odd,} \end{cases}$$

where, in each, k takes the values $2, 4, \dots, m-1$. These sums of like powers of odd or even numbers are expressed by the same function of Bernoullian numbers. For $m=1$, the first formula becomes that by Glaisher,⁶⁴ republished.⁶⁷ Three further G_n formulas are given, but not applied to σ_n .

J. Hammond¹¹¹ wrote $(n; m) = 1$ or 0 according as n/m is integral or fractional, also $\tau(x) = \sigma(x) = 0$ if x is fractional, and stated that

$$\tau(n/m) = \sum_{j=1}^{\infty} (n; jm), \quad \sigma(n/m) = \sum_{j=1}^{\infty} j(n; jm).$$

¹¹¹Messenger Math., 20, 1890-1, 158-163.

From the sum of Euler's $\phi(d)$ for the divisors d of n , he obtained

$$\sigma(n) = \sum_{j=1}^n \tau\left(\frac{n}{j}\right) \phi(j), \quad n\tau(n) = \sum_{j=1}^n \sigma\left(\frac{n}{j}\right) \phi(j).$$

E. Lucas¹¹² proved the last formulas, the result of Cesàro,⁴⁴ and the related one $\sigma(n) + s_n = s_{n-1} + 2n - 1$.

A. Berger¹¹³ considered the mean of the number of decompositions of $1, 2, \dots, x$ into three or more factors, and gave long expressions for $\psi(1) + \dots + \psi(n)$, where $\psi(k) = \sum d^s d_1^{s_1}$, summed for the solutions of $dd_1 = k$. He gave (pp. 116–125) complicated results on the mean value of $\sigma_k(n)$.

D. N. Sokolov and D. T. Egorov^{113a} proved, by use of Bougaief's formulas for sums extending over all the divisors of a number, the formulas in Liouville's²⁵⁻²⁹ series of four articles.

J. W. L. Glaisher¹¹⁴ gave Zeller's⁶⁶ formula and

$$P(n-1) + 2^2P(n-2) - 5^2P(n-5) - 7^2P(n-7) + \dots \\ = \frac{-1}{12} \{5\sigma_3(n) - (18n-1)\sigma(n)\},$$

where $1, 2, 5, \dots$ are pentagonal numbers $(3r^2 \pm r)/2$ and $P(0) = 1$.

Glaisher¹¹⁵ proved formulæ which are greatly shortened by setting $a_{ij}(n) = n^i \sigma_j(n) - 3(n-1)^i \sigma_j(n-1) + 5(n-3)^i \sigma_j(n-3) - 7(n-6)^i \sigma_j(n-6) + \dots$

Write a_{ij} for $a_{ij}(n)$. Besides the formula [of Halphen⁴⁰] $a_{01} = 0$, he gave

$$a_{03} - 2a_{11} = 0, \quad a_{05} - 10a_{13} + \frac{40}{3}a_{21} = 0,$$

$$a_{07} - \frac{126}{5}a_{15} + \frac{756}{5}a_{23} - 168a_{31} = 0,$$

$$a_{09} - 50a_{17} + 720a_{25} - 3360a_{33} + 3360a_{41} = 0,$$

with the agreement that $\sigma(0) = n/3$ and

$$\sigma_3(0) = \frac{-t^2+1}{240}, \quad \sigma_5(0) = \frac{t^3-1}{504}, \quad \sigma_7(0) = \frac{-t^4+1}{480}, \quad \sigma_9(0) = \frac{t^5-1}{264},$$

where $t = 8n + 1$, but did not find the general formula of this type. Next, he gave five formulas of another set, the first one being that of his earlier paper,⁶⁴ the second involving the same function of σ_3 with added terms in $r\sigma(r)$. Finally, denoting Euler's formula (2) by $E\sigma(n) = 0$, it is shown that

$$5E\sigma_3(n) - 18E\{n\sigma(n)\} = 0.$$

Glaisher¹¹⁶ showed that his⁷⁶ third formula holds for all odd numbers v not expressible as a sum of three squares and hence in particular for the

¹¹²Théorie des nombres, 1891, 403–6, 374, 388.

¹¹³Nova Acta Soc. Upsal., (3), 14, 1891 (1886), No. 2, p. 63.

^{113a}Math. Soc. Moscow, 16, 1891, 89–112, 236–255.

¹¹⁴Messenger Math., 21, 1891–92, 47–8.

¹¹⁵Ibid., 49–69.

¹¹⁶Ibid., 122, 126. The further results are quoted in the chapter on sums of three squares.

former case $v \equiv 7 \pmod{8}$. Also the left member of the third formula equals

$$4\{E(v-1) - 3E(v-9) + 5E(v-25) - \dots\}$$

when v is odd, provided $E(0) = 1/4$. If $\Delta'(n)$ denotes the sum of those divisors of n whose complementary divisors are odd,

$$\Delta'(n) - 2\Delta'(n-1) + 2\Delta'(n-4) - 2\Delta'(n-9) + \dots = 0 \text{ or } (-1)^{n-1}n,$$

according as n is not or is a square. [Cf. Lipschitz.⁸⁴] Since $\Delta'(n) = \sigma(n)$ for n odd, we deduce a formula involving σ 's and Δ 's.

M. Lerch¹¹⁷ proved (11) and

$$\sum_{k=1}^n \sigma_s(k) = \Sigma k^s \left[\frac{n}{k} \right], \quad \Sigma F(k) = \Sigma f(k) \left[\frac{n}{k} \right],$$

if $F(n) = \Sigma f(d)$, d ranging over the divisors of n .

K. Th. Vahlen¹¹⁸ proved Liouville's²³ formula and Jacobi's¹⁰ result.

A. P. Minin¹¹⁹ proved that 2, 8, 9, 12, 18, $8q$ and $12p$ (where q is a prime > 2 , p a prime > 3) are the only numbers such that each is divisible by the number of its divisors and the quotient is a prime. Minin¹²⁰ found that 1, 3, 8, 10, 18, 24 and 30 are the only numbers N for which the number of divisors equals the number of integers $< N$ and prime to N .

M. Lerch¹²¹ considered the number $\chi(a, b)$ and sum $X(a, b)$ of the divisors $\leq b$ of a , proved his¹⁰⁰ final formula (17) and

$$(18) \quad \begin{aligned} \sum_{a=1}^c X(m-an, a) &= \sum_{a=1}^c a \{ \chi(m-an, n) - \psi(m-an, a) \}, \\ \sum_{a=0}^c \psi\left(m-an, \frac{a}{r}\right) &= \sum_{a=0}^c \chi(m-an, rn), \quad c \equiv \left[\frac{m-1}{n} \right]. \end{aligned}$$

If δ ranges over the divisors of n ,

$$\begin{aligned} \frac{1}{n} \sum_{a=0}^{n-1} \tau\{(a-am, n)\} &= \Sigma \frac{(\delta, m; a)}{\delta}, & \frac{1}{n} \sum_{a=0}^{n-1} \sigma\{(a-am, n)\} &= \Sigma(\delta, m; a), \\ \sum_{a=1}^n (am, n) &= n \Sigma \frac{\phi(\delta)}{\delta} \cdot (\delta, (m, n)). \end{aligned}$$

He quoted (p. 8) from a letter to him from Chr. Zeller that $\sum_{a=1}^{m-1} a\psi(m-a, a)$ equals the sum of the remainders obtained on dividing m by the integers $< m$.

M. Lerch¹²² proved that

$$\begin{aligned} \Sigma \psi(m+\rho-\sigma n, \sigma) &= \Sigma \chi(m+\rho-\sigma n, n) - \Sigma \left[\frac{m+\rho}{n} - \rho \right], \\ \Sigma \psi(m-\rho-\rho n, \sigma) &= \Sigma \chi(m-\rho-\sigma n, n) - \frac{1}{2} \left[\frac{m-1}{n+1} \right] \cdot \left[\frac{m+n}{n+1} \right], \end{aligned}$$

¹¹⁷Casopis, Prag, 21, 1892, 90-95, 185-190 (in Bohemian). Cf. Jahrbuch Fortschritte Math., 24, 1892, 186-7.

¹¹⁸Jour. für Math., 112, 1893, 29.

¹¹⁹Math. Soc. Moscow, 17, 1893, 240-253.

¹²⁰Ibid., 17, 1894, 537-544.

¹²¹Prag Sitzungsberichte (Math.), 1894, No. 11.

¹²²Ibid., No. 32.

summed for $\rho, \sigma = 0, 1, \dots$, with $\rho \leq \sigma$. Also,

$$\begin{aligned}\sum_{a=0}^{m-1} (-1)^a \psi(m-a, a) &= 2 \sum_{a=0}^{m-1} (-1)^a \Theta'(m-a) + (-1)^m m, \\ \sum_{a=0}^{m-1} \psi'(m-a, a) &= \sum_{k=1}^m (-1)^{k-1} \left[\frac{m}{k} \right], \\ \sum_{a=0}^{m-1} \psi_0(m-a, 2a) &= m + \frac{(-1)^{[\sqrt{m}]} - 1}{2} + 2 \sum_{\nu=1}^m (-1)^\nu \left[\frac{m-\nu^2}{2\nu} \right],\end{aligned}$$

where $\Theta'(k)$ is the number of odd divisors of k ; $\psi'(n, a)$ is the number of divisors $> a$ of n whose complementary divisors are odd; while $\psi_0(k, \mu)$ is the number of even divisors $> \mu$ of k .

In No. 33, he expressed in terms of greatest integer functions

$$\sum_{\rho, \sigma} \{ \psi(m-\rho-\sigma n, k+\sigma) - \chi(m-\rho-\sigma n, n) \},$$

$$\sum_a \{ \psi(m-a, k+a) - (k+a) \psi(m-a, k+a) \}.$$

E. Busche¹²³ gave a geometrical proof of Meissel's²² (11).

J. Schröder¹²⁴ obtained (11) and the first relation (15) of Lerch⁹³ as special cases of the theorem that

$$\sum_{\substack{0, 1, 2, \dots \\ \rho_1, \dots, \rho_m =}} \psi_{r\nu+s}(n-r \sum_{i=1}^m i \rho_i, \sum_{i=1}^m \rho_i)$$

equals the coefficient of x^n in the expansion of

$$\frac{1 - \prod_{i=0}^{m-1} (1 - x^{r^{i+s}})}{(1 - x^{r^m}) \prod_{i=0}^{m-1} (1 - x^{r^{i+s}})},$$

where $\psi_{r\nu+s}(a, \beta)$ is the number of divisors of a which are $> \beta$ and have a complementary divisor of the form $r\nu+s$ ($\nu = 0, 1, \dots$). He obtained

$$\sum_{\rho=0}^{0, 1, \dots} \psi_{r\nu+1}(n-r\rho, \rho) = \left[\frac{n+r-1}{r} \right].$$

Schröder¹²⁵ determined the mentioned coefficient of x^n .

Schröder¹²⁶ proved the generalization of (11):

$$\sum_{\rho=1}^n \left[\frac{n}{\rho} \right]^r = \sum_{\rho=1}^r \left[\frac{n}{\rho} \right]^r + \sum_{\rho=2}^r \{ \rho^r - (\rho-1)^r \} \left[\frac{n}{\rho} \right] + n - \nu^{r+1}, \quad \nu = [\sqrt[n]{n}].$$

For $\sigma(1) + \dots + \sigma(n)$, Dirichlet,¹⁷ end, he gave the value

$$\sum_{s=1}^n s \left[\frac{n}{s} \right] = \frac{1}{2} \sum_{\rho=1}^r \left\{ \left[\frac{n}{\rho} \right]^2 + (2\rho+1) \left[\frac{n}{\rho} \right] \right\} - \frac{1}{2} \nu(\nu+1).$$

E. Busche¹²⁷ proved that if $X = \phi(m)$ is an increasing (or decreasing) function whose inverse function is $m = \Phi(X)$, the divisors of the natural

¹²³Mittheilungen Math. Gesell. Hamburg, 3, 1894, 167-172.

¹²⁴*Ibid.*, 177-188.

¹²⁵*Ibid.*, 3, 1897, 302-8.

¹²⁶*Ibid.*, 3, 1895, 219-223.

¹²⁷*Ibid.*, 3, 1896, 239-40.

numbers between $\phi(m)$ and a , including the limits, are the numbers x from 1 to a (or those $\geq a$) each taken $\xi = [\Phi(x)/x]$ times, and the numbers within the limits which are multiples of x are $x, 2x, \dots, \xi x$. For example, if $a=3$, $\phi(m)=900/m^2$, then $\Phi(x)=30/\sqrt{x}$ and it is a question of the divisors of $3, \dots, 17$; for $x=3$, $\xi=5$ and 3 is a divisor of 3, 6, 9, 12, 15. For $\Phi(x)=n$, $a=1$, the theorem states that among the divisors of $1, \dots, n$ any one x occurs $[n/x]$ times and that these divisors are $1, \dots, n; 1, \dots, [n/2]; 1, \dots, [n/3];$ etc. Hence the sum of the divisors of $1, \dots, n$ is

$$\sum_{x=1}^n x \left[\frac{n}{x} \right] = \frac{1}{2} \sum_{x=1}^n \left\{ \left[\frac{n}{x} \right]^2 + \left[\frac{n}{x} \right] \right\}$$

and their product is

$$\prod_{x=1}^n x^{[n/x]} = \prod_{x=1}^n [n/x]!$$

He proved (pp. 244-6) that the number of divisors $\equiv r \pmod{s}$ of $1, 2, \dots, n$ equals $A+B$, where A is the number of integers $[n/x]$ for $x=1, \dots, n$ which have one of the residues $r, r+1, \dots, s-1 \pmod{s}$, and B is the number of all divisors of $1, 2, \dots, [n/s]$. The number of the divisors δ of m , such that

$$\sqrt{\frac{m}{n}} \leq \delta \leq n$$

and such that δ^2 divides m/δ , equals the number of divisors of $1, 2, \dots, n$. The number of primes among $n, [n/2], \dots, [n/n]$ equals the number of those divisors of $1, \dots, n$ which are primes decreased by the number of divisors which exceed by unity a prime.

P. Bachmann¹²⁸ gave an exposition of the work of Dirichlet,^{14, 17} Mertens,³⁷ Hermite,⁵⁷ Lipschitz,⁵⁸ Cesàro,⁶⁰ Gegenbauer,⁷⁷ Busche,^{123, 127} Schröder.^{124, 126}

N. V. Bougaief¹²⁹ stated that

$$n + \sum d \left[\frac{n}{d-1} \right] = \sum_{j=1}^n X \left(n, 1 + \left[\frac{n}{j} \right] \right), \quad \nu + \sum \left[\sqrt{\frac{n}{d-1}} \right] = \sum_{j=1}^n \chi \left(n, 1 + \left[\frac{n}{j^2} \right] \right),$$

where d ranges over the divisors > 1 of n , and $\nu = [\sqrt{n}]$;

$$\sum d \left[\frac{n}{d^2} \right] = \sum_{j=1}^n X \left(n, \left[\sqrt{\frac{n}{j}} \right] \right),$$

where d ranges over the divisors of n for which $d^2 < n$. If θ is any function,

$$n \sum \frac{n}{d} \theta(d) = \sum_{j=1}^n \sum_d \theta(d),$$

where, on the left, d ranges over all the divisors of n ; on the right, only over those $\leq [n^2/j]$. For $\theta(d) \equiv 1$, this gives

$$n\sigma(n) = \sum_{j=1}^n \chi \left(n, \left[\frac{n^2}{j} \right] \right).$$

¹²⁸Die Analytische Zahlentheorie, 1894, 401-422, 431-6, 490-3.

¹²⁹Comptes Rendus Paris, 120, 1895, 432-4. He used $\xi(a, b)$, $\xi_1(a, b)$ with the same meaning as $\chi(b, a)$, $X(b, a)$ of Lerch,¹²¹ and $\xi_1(n)$ for $\sigma(n)$.

M. Lerch¹³⁰ proved relations of the type

$$\sum_{k=1}^m \chi(k, a) = a \left[\frac{m}{a} \right] + \sum_{k=1}^m \psi \left(k, \frac{m}{a} \right).$$

The number of solutions of $[n/x] = [n/(x+1)]$, $x < n$, is

$$\sum_{r \geq k} \psi(n-r, r) + \sum_{\rho < k} \chi(n-\rho, \rho) \quad (k \equiv -\frac{1}{2} + \sqrt{n+1/4}).$$

F. Nachtikal¹³¹ gave an elementary proof of (15).

M. Lerch¹³² proved that

$$\sum_{\sigma > r s a} \left\{ \psi \left(m - \sigma a, \frac{\sigma}{r} \right) + \psi(m - \sigma a, r a) \right\}$$

remains unaltered if we interchange r and s . He proved (18) and showed that it also follows from the special case (17). From (17) for $n=2$ he derived

$$\sum_{a=0}^c \psi(m-2a, a) = \frac{3m+1}{4} + (-1)^m \frac{m-1}{4}, \quad c \equiv \left[\frac{m-1}{2} \right].$$

L. Gegenbauer^{132a} proved a formula which includes as special cases four of the five general formulas by Bougaief.¹²⁹ When x ranges over a given set S of n positive integers, the sum $\sum f(x)[\chi(x)]$ is expressed as sums of expressions $\Phi(\rho)$ and $\Phi_1(\rho)$, where ρ takes values depending upon x , while $\Phi(z)$ is the sum of the values of $f(x)$ for x in S and $x \geq z$, and $\Phi_1(z)$ is the analogous sum with $x \leq z$.

F. Rogel¹³³ differentiated repeatedly the relation

$$\prod_{\omega=1}^{\infty} (1-x^{\omega})^{\omega^{n-1}} = e^{-T}, \quad T \equiv \sum_{\omega=1}^n \sigma_n(\omega) \frac{x^{\omega}}{\omega}, \quad |x| < 1,$$

then set $x=0$ and found that

$$\sum_{i=1}^r \sum_{a_1! \dots a_r!} \frac{(-1)^i}{\left[\frac{\sigma_n(2)}{2} \right]^{a_2} \dots \left[\frac{\sigma_n(r)}{r} \right]^{a_r}} = \sum_{i=1}^r \sum_{a_1! \dots a_r!} (-1)^i \binom{1}{a_1} \binom{2^{n-1}}{a_2} \dots \binom{r^{n-1}}{a_r},$$

the summations extending over all sets of a 's for which

$$a_1 + a_2 + \dots + a_r = i, \quad a_1 + 2a_2 + \dots + ra_r = r.$$

Starting with the reciprocals of the members of the initial relation, he obtained similarly a second formula; subtracting it from the former result, he obtained

$$\sigma_n(r) = r^n + \frac{1}{2} \sum_{i=3}^r \sum_{j=2}^{r-3} \left\{ \prod_{a_j} (a_j + j^{n-1} - 1) - (-1)^i \prod_{j=1}^{r-3} \binom{j^{n-1}}{a_j} \right\} \\ - \sum \Sigma' \frac{1}{a_1! \dots a_{r-3}!} \prod_{j=2}^{r-3} \left\{ \frac{\sigma_n(j)}{j} \right\}^{a_j},$$

¹³⁰Casopis, Prag, 24, 1895, 25-34, 118-124; 25, 1896, 228-30.

¹³¹Ibid., 25, 1896, 344-6.

¹³²Jornal de Sciencias Math. e Astr. (Teixeira), 12, 1896, 129-136.

^{132a}Monatshefte Math. Phys., 7, 1896, 26.

¹³³Sitzungsber. Gesell. Wiss. (Math.), Prag, 1897, No. 7, 9 pp.

where $i=3, 5, 7, \dots$ in Σ' , while the a 's range over the solutions of

$$a_1 + \dots + a_{r-3} = i, \quad a_1 + 2a_2 + \dots + (r-3)a_{r-3} = r.$$

The case $n=0$ leads to relations for $\tau(r)$.

J. de Vries^{133a} proved the first formula of Lerch's.¹¹⁷

A. Berger¹³⁴ considered the excess $\psi(k)$ of the sum of the odd divisors of k over the sum of the even divisors and proved that

$$\psi(n) + \psi(n-1) + \psi(n-3) + \psi(n-6) + \psi(n-10) + \dots = 0 \text{ or } n,$$

according as n is not or is a triangular number; also Euler's (2).

J. Franel¹³⁵ employed two arbitrary functions f, g and set

$$\theta(n) = \sum f(d)g\left(\frac{n}{d}\right), \quad F(n) = \sum_{j=1}^n f(j), \quad G(n) = \sum_{j=1}^n g(j),$$

where d ranges over the divisors of n . Then

$$\sum_{j=1}^n \theta(j) = \sum_{r=1}^{\nu} f(r)G\left[\frac{n}{r}\right] + \sum_{r=1}^{\nu} g(r)F\left[\frac{n}{r}\right] - F(\nu)G(\nu),$$

where $\nu = [\sqrt{n}]$. The case $f(x) = g(x) = 1$ gives Meissel's²² (11). Next, he evaluated $\sum \vartheta(j)$, where $\vartheta(n) = \sum f(x)g(y)h(z)$, summed for the sets of positive integral solutions of $xyz = n$. In particular, $\vartheta(n)$ is the number of such sets if $f = g = h = 1$. Using Dirichlet's series, it is shown (p. 386) that

$$\sum_{j=1}^n \vartheta(j) = \frac{n}{2} \{ (\log n + 3C - 1)^2 - 3C^2 + 6C_1 + 1 \} + \epsilon,$$

where ϵ is of the order of magnitude of $n^{2/3} \log n$, C is Euler's constant and $C_1 = 0.0728 \dots$ [Piltz,⁵² Landau¹³⁷].

Franel¹³⁶ proved that

$$\sum_{r=1}^p \frac{\tau(r)}{r} = \frac{1}{2} \log^2 p + 2C \log p + \epsilon + A_0,$$

where A_0 is a coefficient in a certain expansion, and $\epsilon p^{1/2}$ remains in absolute value inferior to a fixed number for every p .

E. Landau¹³⁷ gave an immediate proof of (11) and of

$$\sum_{\nu=1}^x T_3(\nu) = \sum_{\nu=1}^x \tau(\nu) \left[\frac{x}{\nu} \right],$$

where $T_3(\nu)$ is the number of decompositions of ν into three factors. He obtained by elementary methods a formula yielding the final result of Franel¹³⁵ on $\sum T_3(\nu)$.

R. D. von Sterneck^{137a} proved Jacobi's¹⁰ formula for s^3 .

^{133a}K. Akad. Wetenschappen te Amsterdam, Verslagen, 5, 1897, 223.

¹³⁴Nova Acta Soc. Sc. Upsaliensis, (3), 17, 1898, No. 3, p. 26.

¹³⁵Math. Annalen, 51, 1899, 369-387.

¹³⁶*Ibid.*, 52, 1899, 536-8.

¹³⁷*Ibid.*, 54, 1901, 592-601.

^{137a}Sitzungsber. Ak. Wiss. Wien (Math.), 109, IIa, 1900, 31-33.

J. Franel¹³⁸ stated that, if $f(n)$ is the number of positive integral solutions of $x^a y^b = n$, where a, b are distinct positive integers,

$$\sum_{r=1}^n f(r) = \zeta\left(\frac{b}{a}\right) n^{\frac{1}{a}} + \zeta\left(\frac{a}{b}\right) n^{\frac{1}{b}} + O\left(n^{\frac{1}{a+b}}\right),$$

where⁹⁰ $O(s)$ is of the order of magnitude of s . Taking $a=1, b=2$, we see that $f(n)$ is the number of divisors of q , where q^2 is the greatest square dividing n , and that the mean of $f(n)$ is $\pi^2/6$.

E. Landau¹³⁹ proved the preceding formula of Franel's.

Elliott⁹⁶ of Ch. V gave formulas involving $\sigma(n)$ and $\tau(n)$.

L. Kronecker¹⁴⁰ proved that the sum of the odd divisors of a number equals the algebraic sum of all its divisors taken positive or negative according as the complementary divisor is odd or even (attributed to Euler²); proved (pp. 267-8) the result of Dirichlet¹⁵ and (p. 345) proved (7) and found the median value (Mittelwert) of $\tau(n)$ to be $\log_e n + 2C$ with an error of the order of magnitude of $n^{-1/4}$ when the number of values employed is of the order of $n^{3/4}$. Calling a divisor of n a smaller or greater divisor according as it is less than or greater than \sqrt{n} , he found (pp. 343-369) the mean and median value of the sum of all smaller (or greater) divisors of $1, 2, \dots, N$ [cf. Gegenbauer⁷⁷], the sum of their reciprocals, and the sum of their logarithms. The mean of Jacobi's¹¹ $E(n)$ is $\pi/4$ (p. 374).

J. W. L. Glaisher¹⁴¹ tabulated for $n=1, \dots, 1000$ the values of the function¹⁰⁴ $H(n)$ and of the excess $J(n)$ of the number of divisors of n which are of the form $8k+1$ or $8k+3$ over the number of divisors of the form $8k+5$ or $8k+7$. When n is odd, $2J(n)$ is the number of representations of n by $x^2 + 2y^2$.

J. W. L. Glaisher¹⁴² derived from Dirichlet's¹⁷ formula, and also independently, the simpler formula

$$\sum_{s=1}^n \left[\frac{n}{s} \right] g(s) = -\rho G(\rho) + \sum_{s=1}^{\rho} \left[\frac{n}{s} \right] g(s) + \sum_{s=1}^{\rho} G \left\{ \left[\frac{n}{s} \right] \right\},$$

where $\rho = [\sqrt{n}]$. The case $g(s) = 1$ gives Meissel's²² formula (11), which is applied to find asymptotic formulæ involving $n/s - [n/s]$. The error of the approximation (7) is discussed at length (pp. 38-75, 180-2). The first formula above is applied (pp. 183-229) to find exact and asymptotic formulas for $\sum f(s)$, when $f(n)$ is Jacobi's¹¹ $E(n)$, Glaisher's¹⁴¹ $H(n)$ or $J(n)$, or the excess $D(n)$ of the number of odd divisors of n over the number of even divisors, or more general functions (p. 215, p. 223) involving the number of divisors with specified residues modulo r .

G. Voronoi¹⁴³ proved a formula like Dirichlet's¹⁷ (7), but with ϵ now of the same order of magnitude as $\sqrt[3]{n} \log_e n$.

¹³⁸L'intermédiaire des math., 6, 1899, 53; 18, 1911, 52-3.

¹³⁹Ibid., 20, 1913, 155.

¹⁴⁰Vorlesungen über Zahlentheorie, I, 1901, 54-55.

¹⁴¹Messenger Math., 31, 1901-2, 64-72, 82-91.

¹⁴²Quar. Jour. Math., 33, 1902, 1-75, 180-229.

¹⁴³Jour. für Math., 126, 1903, 241-282.

H. Mellin¹⁴⁴ obtained asymptotic expressions for $\Sigma \tau(n)$, $\Sigma \sigma(n)$.

I. Giulini¹⁴⁵ noted that, if m and h are given integers, and $\beta(r)$ is the sum of the divisors $d = mk + h$ of r , then

$$\beta(1) + \dots + \beta(n) = \sum_k d[n/d], \quad k = 0, 1, \dots, [(n-h)/m].$$

The number and sum of the divisors $d = mk + h$ of $1, \dots, n$ are

$$\sum_{k=0}^{[(n-h)/m]} \left[\frac{n}{d} \right], \quad m \sum_{r=1}^{[n/(m+h)]} E_2 \left(\frac{n-hr}{mr} \right) + h \sum_{s=1}^{[n/h]} \left[\frac{n-sh}{ms} + 1 \right],$$

respectively, where $E_2(x) = [x][x+1]/2$.

G. Voronoi^{145a} gave for $T(x)$ the precise analytic expression

$$x(\log x + 2C - 1) + \frac{1}{4} + \frac{1}{2}\tau(x) - 2 \int_x^\infty g(t) dt + \int_0^\infty \{g(-x+ti) - g(-x-ti)\} i dt,$$

and (p. 515) approximations to these integrals, where

$$g(x) = -\frac{1}{4} \log x - \frac{1}{2}C - \frac{\log 4\pi^2 x}{4\pi^2 x} + \frac{1}{2\pi^2} \sum_{n=1}^\infty \tau(n) \log \frac{x}{n} \left(\frac{1}{x-n} + \frac{1}{x+n} \right).$$

He discussed at length the function $g(x)$ and (pp. 467, 480-514) the asymptotic value of $\Sigma \tau(n)(x-n)^k/k!$.

J. Schröder¹⁴⁶ proved that the sum of the ν th powers of $1, \dots, n$ is

$$\sum_{\rho=1}^n \rho^\nu \left[\frac{n}{\rho} \right] = n\sigma_{\nu-1}(n) + \sum_{\rho=t+1}^{n-1} \rho^\nu + \sum_{\rho=1}^t \rho^\nu \left[\frac{n}{\rho} \right],$$

where $t = [n/2]$, and the accent on the last Σ denotes that the summation extends only over the values $\leq t$ of ρ which are not divisors of n .

E. Busche¹⁴⁷ proved that, if we multiply each divisor of m by each divisor of n , the number of times we obtain a given divisor a of mn is $\tau(\mu\nu/a)$, where μ is the g. c. d. of m, a , and ν is that of n, a . A like theorem is proved for the divisors of $mnp \dots$. He stated (p. 233; cf. Bachmann¹⁶⁸) that

$$\sigma_h(m)\sigma_h(n) = \sum d^h \sigma_h \left(\frac{mn}{d^2} \right),$$

where d ranges over the common divisors of m, n .

C. Hansen¹⁴⁸ denoted by $T_1(n)$ and $T_3(n)$ the number of divisors of n of the respective forms $4k-1$ and $4k-3$, and set

$$A_n = T_3(4n-3) - T_1(4n-3).$$

By use of Jacobi's $\theta_3(\nu, s)$ for $\nu = 1/4$, he proved that

$$\sum_{n=1}^\infty A_n s^{4n-3} = \sum_{n=1}^\infty (-1)^{n+1} \frac{s^{2n-1}}{1-s^{4n-2}} = \frac{s-3s^9+5s^{25}-\dots}{1-2s^4+2s^{16}+\dots},$$

¹⁴⁴Acta Math., 28, 1904, 49.

¹⁴⁵Giornale di mat., 42, 1904, 103-8.

^{145a}Annales sc. l'école norm. sup., (3), 21, 1904, 213-6, 245-9, 258-267, 472-480. Cf. Hardy.¹⁸⁰

¹⁴⁶Mitt. Math. Gesell. Hamburg, 4, 1906, 256-8.

¹⁴⁷Ibid., 4, 1906, 229.

¹⁴⁸Oversigt K. Danske Videnskabernes Selskabs Forhandling, 1906, 19-30 (in French).

and hence deduced the law of a recursion formula for A_n . The law of a recursion formula for $B_n = 4\{T_3(n) - T_1(n)\}$ is obtained from

$$\sum_{n=0}^{\infty} B_n s^{8n} \sum_{n=0}^{\infty} s^{(2n+1)^2} \cos(2n+1) \frac{\pi}{4} = \sum_{n=0}^{\infty} (2n+1) s^{(2n+1)^2} \sin(2n+1) \frac{\pi}{4},$$

with $B_0 = 1$, which was found by use of Jacobi's $\theta(\frac{1}{4}, s)$. Next,

$$\Phi(s) \equiv \sum_{n=1}^{\infty} \frac{s^n}{1+s^{2n}} = \frac{1}{4} \sum_{n=1}^{\infty} B_n s^n$$

is shown to satisfy the functional equation

$$\Phi(is) = \frac{i}{2} \{\Phi(s) - \Phi(-s)\} - \Phi(s^2) + 2\Phi(s^4).$$

If a convergent series $\sum c_n s^n$ is a solution $\Phi(s)$ of the latter, the coefficients are uniquely determined by the c_{4k-3} ($k = 1, 2, \dots$), which are arbitrary. Hence the function B_n is determined for all values of n by its values for $n = 4k - 3$ ($k = 1, 2, \dots$).

S. Wigert¹⁴⁹ proved that, for sufficiently large values of n , $\tau(n) < 2^t$, where $t = (1 + \epsilon) \log n \div \log \log n$, for every $\epsilon > 0$; while there exist certain values of n above any limit for which $\tau(n) > 2^s$, $s = (1 - \epsilon) \log n \div \log \log n$.

J. V. Pexider¹⁵⁰ proved that, if a, n are positive, a an integer,

$$\sum_{k=1}^{[n]} \left[\frac{n}{k} \right] = \sum_{k=1}^a \left[\frac{n}{k} \right] + \sum_{k=1}^{[n/a]} \left[\frac{n}{k} \right] - a \left[\frac{n}{a} \right],$$

by the method used, for the case in which n is an integral multiple of a , by E. Cesàro.⁶⁰ Taking $a = [\sqrt{n}]$, we have the second equation (11). Proof is given of the first equation (11) and

$$\sum k \left[\frac{n}{k} \right] = \sum \sigma(k), \quad \sum \left[\frac{n}{d} \right] \left[\frac{n-1}{d} \right] = \sum d^2 - \sigma[n],$$

where d ranges over the divisors of $[n]$.

O. Meissner¹⁵¹ noted that, if $m = p_1^{e_1} \dots p_n^{e_n}$, where p_1 is the least of the distinct primes p_1, \dots, p_n , then

$$\prod_{i=1}^n \frac{p_i}{p_i - 1} > \frac{\sigma(m)}{m} > \prod_{i=2}^n \frac{p_i}{p_i - 1}, \quad 1 < \frac{\sigma(m)}{m \log m} < G,$$

where G is finite and independent of m . If $k > 1$, $\sigma_k(m)/m^k$ is bounded.

W. Sierpinski¹⁵² proved that the mean of the number of integers whose squares divide n , of their sum, and of the greatest of them, are

$$\frac{\pi^2}{6}, \quad \frac{1}{2} \log n + \frac{3}{2} C, \quad \frac{3}{\pi^2} \log n + \frac{9C}{\pi^2} + \frac{36}{\pi^4} \sum_{s=1}^{\infty} \frac{\log s}{s^2},$$

respectively, where C is Euler's constant.

J. W. L. Glaisher¹⁵³ derived formulas differing from his¹¹⁰ earlier ones only in the replacement of d by $(-1)^{d-1}d$, i. e., by changing the sign of each

¹⁴⁹Arkiv för mat., ast., fys., 3, 1906-7, No. 18, 9 pp.

¹⁵⁰Rendiconti Circolo Mat. Palermo, 24, 1907, 58-63.

¹⁵¹Archiv Math. Phys., (3), 12, 1907, 199.

¹⁵²Sprawozdania Tow. Nank. (Proc. Sc. Soc. Warsaw), 1, 1908, 215-226 (Polish).

¹⁵³Proc. London Math. Soc., (2), 6, 1908, 424-467.

even divisor d . In the case of the theorems on the cancellation of actual divisors, the results follow at once from the earlier ones. But the recursion formulæ for σ_n and ζ_n are new and too numerous to quote. Cancellation formulas (pp. 449–467) are proved for the divisors whose complementary divisors are odd, and applied to obtain recursion formulæ for the related function $\Delta_r'(n)$ of Glaisher.^{74, 87}

E. Landau¹⁵⁵ proved that $\log 2$ is the superior limit for $x = \infty$ of $\log \tau(x) \cdot \log \log x \div \log x$.

M. Fekete¹⁵⁶ employed the determinant $R_{k,n}^{(t)}$ obtained by deleting the last t rows and last t columns of Sylvester's eliminant of $x^k - 1 = 0$ and $x^n - 1 = 0$. Set, for $k \leq n$,

$$b_n(k) = 1 - |R_{k,n}^{(k-1)}|, \quad c_n(i, k) = |R_{i,k}^{(1)}| (1 - |R_{k,n}^{(k-1)}|) (1 - |R_{i,n}^{(i-1)}|) (1 - |R_{ik,n}^{(ik-1)}|).$$

Then $b_n(k) = 1$ or 0 according as k is or is not a divisor of n ; while $c_n(i, k) = 1$ if $ik = n$ and i is relatively prime to k , but $= 0$ in the contrary cases. Thus

$$\tau(n) = \sum_{k=1}^n b_n(k), \quad \sigma(n) = \sum_{k=1}^n kb_n(k),$$

while the number and sum of those divisors d of n , which are relatively prime to the complementary divisors n/d , equal, respectively,

$$\sum_{i,k=1}^n c_n(i, k), \quad \frac{1}{2} \sum_{i,k=1}^n (i+k) c_n(i, k).$$

J. Schröder¹⁵⁷ deduced from his¹²⁴ final equation the results

$$\sum_{\rho=0,1,\dots} \psi_{rr+s} \left(n - \rho, \left[\frac{\rho}{r} \right] \right) = \left[\frac{n}{s} \right], \quad \Sigma \psi \left(n - \rho, \left[\frac{\rho}{r} \right] \right) = \sum_{s=1}^r \left[\frac{n}{s} \right].$$

The final sum equals $\sum_{s=1}^n \psi(s, [s/(r+1)])$.

P. Bachmann¹⁵⁸ gave an exposition of the work of Euler,^{5, 6} Glaisher,^{63, 64} Zeller,⁶⁶ Stern,⁸⁵ Glaisher,¹¹⁰ Liouville.³⁰

E. Landau¹⁵⁹ proved that the number of positive integers $\leq x$ which have exactly n positive integral divisors is asymptotic to

$$Ax^{1/(p-1)} (\log \log x)^{w-1} / \log x,$$

where p is the least prime factor of n , and p occurs exactly w times in n , while A depends only on n .

K. Knopp¹⁶⁰ obtained, by enumerations of lattice points,

$$\sum_{k=1}^n f_1(q, k) = \sum_{k=1}^n f_2(k, q) = \sum_{k=1}^w f_1(q, k) + \sum_{k=1}^w f_2(k, q) - F(w, w),$$

where $q = [n/k]$ and

$$f_1(r, k) = \sum_{j=1}^r f(j, k), \quad f_2(k, s) = \sum_{j=1}^s f(k, j), \quad F(r, s) = \sum_{j=1}^s f_1(r, j).$$

¹⁵⁵Handbuch... Verteilung der Primzahlen, I, 1909, 219–222.

¹⁵⁶Math. és Phys. Lapok (Math. phys. soc.), Budapest, 18, 1909, 349–370. German transl., Math. Naturwiss. Berichte aus Ungarn, 26, 1913 (1908), 196–211.

¹⁵⁷Mitt. Math. Gesell. Hamburg, 4, 1910, 467–470.

¹⁵⁸Niedere Zahlentheorie, II, 1910, 268–273, 284–304, 375.

¹⁵⁹Annaes Sc. Acad. Polyt. do Porto, Coimbra, 6, 1911, 129–137.

¹⁶⁰Sitzungsber. Berlin Math. Gesell., 11, 1912, 32–9; with Archiv Math. Phys.

Taking $f(h, k) \equiv 1$, we obtain Meissel's²² (11), a direct proof of which is also given. Taking $f(h, k) = f(h)g(hk)$, we get

$$\sum_{k=1}^n \sum_{j=1}^q f(j)g(jk) = \sum_{k=1}^n f(k) \sum_{j=1}^q g(jk), \quad q = \left[\frac{n}{k} \right],$$

special cases of which yield many known formulas involving Möbius's function $\mu(n)$ or Euler's function $\phi(n)$.

E. Landau¹⁶¹ proved the result due to Pfeiffer⁹⁰, and a theorem more effective than that by Piltz⁵², having the O terms replaced by $O(x^\epsilon)$, where, for every $\epsilon > 0$,

$$\alpha = \frac{k-1}{k+1} - \sigma + \epsilon.$$

E. Landau¹⁶² extended the theorem of Piltz⁵² to an arbitrary algebraic domain, defining $T_k(n)$ to be the number of representations of n as the norm of a product of k ideals of the domain.

J. W. L. Glaisher¹⁶³, generalizing his¹⁴² formula, proved that

$$\sum_{s=1}^n F\left[\frac{n}{s}\right]g(s) = \sum_{s=1}^n F\left[\frac{n}{s}\right]g(s) + \sum_{s=1}^n G\left[\frac{n}{s}\right]f(s) - F(\rho)G(\rho),$$

where $F(s) = f(1) + \dots + f(s)$, $G(s) = g(1) + \dots + g(s)$, $\rho = [\sqrt{n}]$. A similar generalization of another formula by Dirichlet¹⁷ is proved, also analogous theorems involving only odd arguments.

Glaisher¹⁶⁴ applied the formulas just mentioned to obtain theorems on the number and sum of powers of divisors, which include all or only the even or only the odd divisors. Among the results are (11) and those of Hacks.^{96, 97} The larger part of the paper relates to asymptotic formulas for the functions mentioned, and the theorems are too numerous to be cited here.

E. Landau⁹¹ gave another proof of the result by Voronoï¹⁴³. He proved (p. 2223) that $\tau(n) < 4n^{1/3}$.

J. W. L. Glaisher¹⁶⁵ stated again many of his¹⁶⁴ results, but without determining the limits of the errors of the asymptotic formulas.

S. Minetola¹⁶⁶ proved that the number of ways a product of m distinct primes can be expressed as a product of n factors is

$$\frac{1}{n!} \left\{ n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \dots \pm \binom{n}{n-1}1^m \right\}.$$

T. H. Gronwall¹⁶⁷ noted that the superior limits for $x = \infty$ of

$$\sigma_\alpha(x)/x^\alpha \quad (\alpha > 1), \quad \sigma(x)/(x \log \log x)$$

are the zeta function $\zeta(\alpha)$ and e^C , respectively, C being Euler's constant.

¹⁶¹Göttingen Nachrichten, 1912, 687-690, 716-731.

¹⁶²Trans. Amer. Math. Soc., 13, 1912, 1-21.

¹⁶³Quar. Jour. Math., 43, 1912, 123-132.

¹⁶⁴*Ibid.*, 315-377. Summary in Glaisher.¹⁶⁵

¹⁶⁵Messenger Math., 42, 1912-13, 1-12.

¹⁶⁶Il Boll. di Matematica Gior. Sc.-Didat., Roma, 11, 1912, 43-46; cf. Giornale di Mat., 45, 1907, 344-5; 47, 1909, 173, §1, No. 7.

¹⁶⁷Trans. Amer. Math. Soc., 14, 1913, 113-122.

P. Bachmann¹⁶⁸ proved the final formula of Busche.¹⁴⁷

K. Knopp¹⁶⁹ studied the convergence of $\sum b_n x^n / (1 - x^n)$, including the series of Lambert⁷, and proved that the function defined in the unit circle by Euler's¹ product (1) can not be continued beyond that circle.

E. T. Bell¹⁷⁰ proved that, if P is the product of all the distinct prime factors of m , and λ is their number, and d ranges over all divisors of m ,

$$6^\lambda \sum \tau(d) \tau\left(\frac{m}{d}\right) = \tau(m) \tau(Pm) \tau(P^2 m).$$

J. F. Steffensen¹⁷¹ proved that,⁹⁰ if lx denotes $\log x$,

$$\sum_1^x \frac{\tau(n)}{n} = \frac{1}{2} l^2 \nu + O(l\nu), \quad \sum_1^x \frac{\sigma(n)}{n^2} = \frac{\pi^2}{6} l\nu + O(1).$$

S. Wigert¹⁷² proved, for the sum $n \cdot s(n)$ of the divisors of n ,

$$(1 - \epsilon) e^C \log \log n < s(n) < (1 + \epsilon) e^C \log \log n,$$

$$\sum_{n \leq x} s(n) = \frac{\pi^2}{6} x - \psi(x), \quad \psi(x) = x \sum_{n > x} \frac{1}{n^2} + \sum_{n \neq x} \frac{1}{n} \rho\left(\frac{x}{n}\right),$$

for $\epsilon > 0$ and $\rho(x) = x - [x]$. For x sufficiently large,

$$\left(\frac{1}{4} - \epsilon\right) \log x < \psi(x) < \left(\frac{3}{4} + \epsilon\right) \log x.$$

Besides results on $\sum s(x)(x - n)^k$, $\sum s(n) \log x/n$, he proved that

$$\sum_{n \leq x} ns(n) = \frac{\pi^2 x^2}{12} + x \left\{ \frac{1}{2} \log x - \psi(x) \right\} + O(x).$$

E. Landau¹⁷³ gave corrections and simplifications in the proofs by Wigert.¹⁷²

E. T. Bell¹⁷⁴ introduced a function including as special cases the functions treated by Liouville,²⁵⁻²⁹ restated his theorems and gave others.

J. G. van der Corput¹⁷⁵ proved, for $\mu(d)$ as in Chapter XIX,

$$\sum_{d=1}^x d^n \mu(d) \sum_{k=1}^{x/d} \sigma_n(k) = x.$$

S. Ramanujan¹⁷⁶ proved that $\tau(N)$ is always less than 2^k and 2^t , where⁹⁰

$$k = \frac{\log N}{\log \log N} + O\left\{ \frac{\log N}{(\log \log N)^2} \right\}, \quad t = Li(\log N) + O\{\log N e^{-a(\log \log N)^{1/2}}\},$$

for $Li(x)$ as in Ch. XVIII, and for a a constant. Also, $\tau(N)$ exceeds 2^k and 2^t for an infinitude of values of N . A highly composite number N is one for which $\tau(N) > \tau(n)$ when $N > n$; if $N = 2^{a_2} 3^{a_3} \dots p^{a_p}$, then $a_2 \geq a_3 \geq a_5 \geq$

¹⁶⁸Archiv Math. Phys., (3), 21, 1913, 91.

¹⁶⁹Jour. für Math., 142, 1913, 283-315; minor errata, 143, 1913, 50.

¹⁷⁰Amer. Math. Monthly, 21, 1914, 130-1.

¹⁷¹Acta Math., 37, 1914, 107. Extract from his Danish Diss., "Analytiske Studier med Anvendelser paa Taltheorien," Kopenhagen, 1912.

¹⁷²Ibid., 113-140.

¹⁷³Göttingische gelehrte Anzeigen, 177, 1915, 377-414.

¹⁷⁴Univ. of Washington Publications Math. Phys., 1, 1915, 6-8, 38-44.

¹⁷⁵Wiskundige Opgaven, 12, 1915, 182-4.

¹⁷⁶Proc. London Math. Soc., (2), 14, 1915, 347-409.

$\dots \geq a_p$, while $a_p = 1$ except when $N = 4$ or 36 . The value of λ for which $a_2 > a_3 > \dots > a_\lambda$ is investigated at length. The ratio of two consecutive highly composite numbers N tends to unity. There is a table of N 's up to $\tau(N) = 10080$. An N is called a superior highly composite number if there exists a positive number ϵ such that

$$\frac{\tau(N_2)}{N_2^\epsilon} < \frac{\tau(N)}{N^\epsilon} \geq \frac{\tau(N_1)}{N_1^\epsilon}$$

for all values of N_1 and N_2 such that $N_2 > N > N_1$. Properties of $\tau(N)$ are found for (superior) highly composite numbers.

Ramanujan¹⁷⁷ gave for the zeta function (12) the formula

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} = \sum_{j=1}^{\infty} j^{-s} \sigma_a(j) \sigma_b(j),$$

and found asymptotic formulæ for

$$\sum_{j=1}^n \tau^s(j), \quad \sum_{j=1}^n \tau(jv+c), \quad \prod_{j=1}^n \sigma_s(j), \quad \sum_{j=1}^n \sigma_a(j) \sigma_1(j), \quad D_v(n),$$

for $a = 0$ or 1 , where

$$D_v(n) = \sum_{j=1}^n \tau(jv) = \sum \mu(d) \tau\left(\frac{v}{d}\right) D_1\left(\frac{n}{d}\right),$$

summed for the divisors d of v . If δ is a common divisor of u, v ,

$$\tau(uv) = \sum_1^{\infty} \mu(n) \tau\left(\frac{u}{n}\right) \tau\left(\frac{v}{n}\right) = \sum \mu(\delta) \tau\left(\frac{u}{\delta}\right) \tau\left(\frac{v}{\delta}\right).$$

E. Landau^{177a} gave another asymptotic formula for the number of decompositions of the numbers $\leq x$ into k factors, $k \geq 2$.

Ramanujan¹⁷⁸ wrote $\sigma_s(0) = \frac{1}{2} \zeta(-s)$ and proved that

$$\begin{aligned} \sum_{j=0} \sigma_r(j) \sigma_s(n-j) &= \frac{\Gamma(r+1) \Gamma(s+1)}{\Gamma(r+s+2)} \cdot \frac{\zeta(r+1) \zeta(s+1)}{\zeta(r+s+2)} \sigma_{r+s+1}(n) \\ &\quad + \frac{\zeta(1-r) + \zeta(1-s)}{r+s} n \sigma_{r+s-1}(n) + O(n^{2(r+s+1)/3}), \end{aligned}$$

for positive odd integers r, s . Also that there is no error term in the right member if $r = 1, s = 1, 3, 5, 7, 11$; $r = 3, s = 3, 5, 9$; $r = 5, s = 7$.

J. G. van der Corput¹⁷⁹ wrote s for the g. c. d. of the exponents a_1, a_2, \dots in $m = \prod p_i^{a_i}$ and expressed in terms of zeta function $\zeta(i)$, $i = 2, \dots, k+1$,

$$\sum_{m=2}^{\infty} \{\sigma_k(s) - 1\} / m$$

if $k > 1$; the sum being $1 - C$ if $k = -1$, where C is Euler's constant.

¹⁷⁷Messenger Math., 45, 1915-6, 81-84.

^{177a}Sitzungsber. Ak. Wiss. München, 1915, 317-28.

¹⁷⁸Trans. Cambr. Phil. Soc., 22, 1916, 159-173.

¹⁷⁹Wiskundige Opgaven, 12, 1916, 116-7.

G. H. Hardy¹⁸⁰ proved that for Dirichlet's¹⁷ formula (7) there exists a constant K such that $\epsilon > Kn^{1/4}$, $\epsilon < -Kn^{1/4}$, for an infinitude of values of n surpassing all limit. In Piltz's⁵² formula

$$\sum_{n=1}^x T_k(n) = x \{a_{k1}(\log x)^{k-1} + \dots + a_{kk}\} + \epsilon_k,$$

$\epsilon_k > Kx^t$, $\epsilon_k < -Kx^t$, where $t = (k-1)/(2k)$. He gave two proofs of an equivalent to Voronoï's^{145a} explicit expression for $T(x)$.

Hardy¹⁸¹ wrote $\Delta(n)$ for Dirichlet's ϵ in (7) and proved that,⁹⁰ for every positive e , $\Delta(n) = O(n^{e+1/4})$ on the average, i. e.,

$$\frac{1}{n} \int_1^n |\Delta(t)| dt = O(n^{e+1/4}).$$

G. H. Hardy and S. Ramanujan¹⁸² employed the phrase "almost all numbers have a specified property" to mean that the number of the numbers $\leq x$ having this property is asymptotic to x as x increases indefinitely, and proved that if f is a function of n which tends steadily to infinity with n , then almost all numbers have between $a-b$ and $a+b$ different prime factors, where $a = \log \log n$, $b = f\sqrt{a}$. The same result holds also for the total number of prime factors, not necessarily distinct. Also a is the normal order of the number of distinct prime factors of n or of the total number of its prime factors, where the normal order of $g(n)$ is defined to mean $f(n)$ if, for every positive ϵ , $(1-\epsilon)f(n) < g(n) < (1+\epsilon)f(n)$ for almost all values of n .

S. Wigert¹⁸³ gave an asymptotic representation for $\sum_{n \leq x} \tau(n)(x-n)^k$.

E. T. Bell¹⁸⁴ gave results bearing on this chapter.

F. Rogel¹⁸⁵ expressed the sum of the r th powers of the divisors $\leq q$ of m as an infinite series involving Bernoullian functions.

A. Cunningham¹⁸⁶ found the primes $p < 10^4$ (or 10^5) for which the number of divisors of $p-1$ is a maximum 64 (or 120).

Hammond⁴³ of Ch. XI and Rogel²⁴³ of Ch. XVIII gave formulas involving σ and τ . Bougaief^{59, 62} of Ch. XIX treated the number of divisors $\leq m$ of n . Gegenbauer⁶⁰ of Ch. XIX treated the sum of the p th powers of the divisors $\geq m$ of n .

¹⁸⁰Proc. London Math. Soc., (2), 15, 1916, 1-25.

¹⁸¹*Ibid.*, 192-213.

¹⁸²Quar. Jour. Math., 48, 1917, 76-92.

¹⁸³Acta Math., 41, 1917, 197-218.

¹⁸⁴Annals of Math., 19, 1918, 210-6.

¹⁸⁵Math. Quest. Educ. Times, 72, 1900, 125-6.

¹⁸⁶Math. Quest. and Solutions, 3, 1917, 65.



CHAPTER XI.

MISCELLANEOUS THEOREMS ON DIVISIBILITY, GREATEST COMMON DIVISOR, LEAST COMMON MULTIPLE.

THEOREMS ON DIVISIBILITY.

An anonymous author¹ noted that for n a prime the sum of $1, 2, \dots, n-1$ taken by twos (as $1+2, 1+3, \dots$), by fours, by sixes, etc., when divided by n give equally often the residues $1, 2, \dots, n-1$, and once oftener the residue 0. The sum by threes, fives, ..., give equally often the residues $1, \dots, n-1$ and once fewer the residue 0.

J. Dienger² noted that if $m^{2r+1} \pm 1$ and $(m^{4r+2} - 1)/(m^2 - 1)$ are divisible by the prime p , then the sum of any $2r+1$ consecutive terms of the set $1, m^{2^n}, m^{2 \cdot 2^n}, m^{3 \cdot 2^n}, \dots$ is divisible by p . The case $m=2, r=1, p=3$ or 7 was noted by Stifel (Arith. Integra).

G. L. Dirichlet³ proved that when n is divided by $1, 2, \dots, n$ in turn the number of cases in which the remainder is less than half the divisor bears to n a ratio which, as n increases, has the limit $2 - \log 4 = 0.6137 \dots$; the sum of the quotients of the n remainders by the corresponding divisors bears to n a ratio with the limit $0.423 \dots$.

Dirichlet⁴ generalized his preceding result. The number h of those divisors $1, 2, \dots, p$ ($p \leq n$), which yield a remainder whose ratio to the divisor is less than a given proper fraction a , is

$$h = \sum_{s=1}^p \left\{ \left[\frac{n}{s} \right] - \left[\frac{n}{s} - a \right] \right\}.$$

Assuming that p^2/n increases indefinitely with n , the limit of h/p is a if n/p increases indefinitely with n , but if n/p remains finite is

$$\frac{n}{p} \int_0^1 \frac{1 - \varphi^a}{1 - \varphi} d\varphi - \frac{n}{p} \sum_{s=1}^q \left(\frac{1}{s} - \frac{1}{s+a} \right) + \left\{ 1 - \frac{n}{p(p+a)} \right\} \left\{ q - \left[\frac{n}{p} - a \right] \right\}, \quad q = \left[\frac{n}{p} \right].$$

J. J. Sylvester⁵ noted that 2^{m+1} is a factor of the integral part of k^{2m+1} and of the integer just exceeding k^{2m} , where $k = 1 + \sqrt{3}$.

N. V. Bougaief⁶ called a number primitive if divisible by no square > 1 , secondary if divisible by no cube. The number of primitive numbers $\leq n$ is

$$H_1(n) = \sum_1^{t_1} q(u) + \sum_1^{t_2} q(u) + \dots, \quad t_i = [\sqrt{n/i}],$$

where $q(u)$ is zero if u is not primitive, but is $+1$ or -1 for a primitive u , according as u is a product of an even or odd number of prime factors.

¹Jour. für Math., 6, 1830, 100-4.

²Archiv Math. Phys., 12, 1849, 425-9.

³Abh. Ak. Wiss. Berlin, 1849, 75-6; Werke, 2, 57-58. Cf. Sylvester, Amer. Jour. Math., 5, 1882, 298-303; Coll. Math. Papers, IV, 49-54.

⁴Jour. für. Math., 47, 1854, 151-4. Berlin Berichte, 1851, 20-25; Werke, 2, 97-104; French transl. by O. Terquem, Nouv. Ann. Math., 13, 1854, 396.

⁵Quar. Journ. Math., 1, 1857, 185. Lady's and Gentleman's Diary, London, 1857, 60-1.

⁶Comptes Rendus Paris, 74, 1872, 449-450. Bull. Sc. Math. Astr., 10, I, 1876, 24. Math. Sbornik (Math. Soc. Moscow), 6, 1872-3, I, 317-9, 323-331.

To obtain the number $H_2(n)$ of secondary numbers $\leq n$, replace square roots by cube roots in the t_i . We have

$$H_1(n) + H_1\left(\left[\frac{n}{2^2}\right]\right) + H_1\left(\left[\frac{n}{3^2}\right]\right) + \dots = n, \quad H_2(n) + H_2\left(\left[\frac{n}{2^3}\right]\right) + \dots = n,$$

and similarly for $H_{\lambda-1}(n)$ given by (2) below.

J. Grolous⁷ considered the probability R_k that a number be divisible by at least one of the integers Q_1, \dots, Q_k , relatively prime by twos, and showed that

$$R_n = \frac{1}{Q_1} + \frac{1}{Q_2}(1 - R_1) + \dots + \frac{1}{Q_n}(1 - R_{n-1}).$$

Chr. Zeller^{7a} modified Dirichlet's⁴ expression for h . The sums

$$\sum_{s=1}^p \left[\frac{n}{s} - a \right], \quad \sum_{s=1}^{p-1} \left[\frac{n}{s+a} \right]$$

are equal. The sum of the terms of the second with $s > \mu = [\sqrt{p}]$ equals the excess of the sum of the first μ terms of the first over μ^2 or $\mu^2 - 1$, the latter in the case of numbers between μ^2 and $\mu^2 + \mu$. Hence we may abbreviate the computation of h .

E. Cesàro⁸ obtained Dirichlet's^{3,4} results and similar ones. The mean (p. 174) of the number of decompositions of N into two factors having p as their g. c. d. is $6(\log N)/(p^2\pi^2)$. The mean (p. 230) of the number of divisors common to two positive integers n, n' is $\pi^2/6$, that of the sum of their common divisors is

$$\frac{1}{2} \log_e nn' + 2C - \frac{\pi^2}{12} + \frac{1}{2},$$

where $C = 0.57721 \dots$. The sum of the inverses of the n th powers of two positive integers is in mean $\zeta(n+2)$ where ζ is defined by (12) of Ch. X.

E. Cesàro⁹ proved the preceding results on mean values; showed that the number of couples of integers whose l. c. m. is n is the number of divisors of n^2 , if (a, b) and (b, a) are both counted when $a \neq b$; found the mean of the l. c. m. of two numbers; found the probability that in a random division the quotient is odd, and the mean of the first or last digit of the quotient; the probability that the g. c. d. of several numbers shall have specified properties.

Cesàro^{9a} noted that the probability that an integer has no divisor > 1 which is an exact r th power is $1/\zeta(r)$.

L. Gegenbauer¹⁰ proved that the number of integers $\leq x$ and divisible by no square is asymptotic to $6x/\pi^2$, with an error of order inferior to \sqrt{x} . He proved the final formulas of Bougaief.⁶

⁷Bull. Sc. Soc. Philomatique de Paris, 1872, 119-128.

^{7a}Nachrichten Gesell. Wiss. Göttingen, 1879, 265-8.

⁸Mém. Soc. R. Sc. de Liège, (2), 10, 1883, No. 6, 175-191, 219-220 (corrections, p. 343).

^{8a}Annali di mat., (2), 13, 1885, 235-351, "Excursions arith. à l'infini."

^{9a}Nouv. Ann. Math., (3), 4, 1885, 421.

¹⁰Denkschr. Akad. Wien (Math.), 49, I, 1885, 47-8. Sitzungsber. Akad. Wien, 112, II a, 1903, 562; 115, II a, 1906, 589. Cf. A. Berger, Nova Acta Soc. Upsal., (3), 14, 1891, Mém. 2, p. 110; E. Landau, Bull. Soc. Math. France, 33, 1905, 241. See Gegenbauer,^{72, 79} Ch. X.

Gegenbauer^{10a} proved that the arithmetical mean of the greatest integers contained in k times the remainders on the division of n by $1, 2, \dots, n$ approaches

$$k \log k + k - 1 - k \sum_{x=1}^{k-1} 1/x$$

as n increases. The case $k=2$ is due to Dirichlet.

Gegenbauer¹¹ gave formulas involving the greatest divisor $t_a(n)$, not divisible by a , of the integer n . In particular, he gave the mean value of the greatest divisor not divisible by an a th power.

L. Gegenbauer,¹² employing Merten's function μ (Ch. XIX) and $R(a) = a - |a|$, gave the three general formulas

$$\begin{aligned} \sum_{x_1}^{r+n} \sum_{y=1}^n \mu\left(\frac{x_1}{y}\right) f(y) &= \sum_{k=1}^{r+n} f(k) - \sum_{k=1}^r f(k) - \sum_{k=1}^n f(k), \\ \sum_{x_2}^{rn} \sum_{y=1}^n \mu\left(\frac{x_2}{y}\right) f(y) &= \sum_{k=(r-1)n+1}^{rn} f(k) - \sum_{k=1}^n f(k), \\ \sum_{x, y=1}^{rn} \mu\left(\frac{x}{y}\right) f(y) \left\{ \frac{1}{n} R\left(\frac{n}{x}\right) - \frac{1}{r} R\left(\frac{r}{x}\right) \right\} &= \frac{1}{r} \sum_{k=1}^r f(k) - \frac{1}{n} \sum_{k=1}^n f(k), \end{aligned}$$

where x_2 ranges over the divisors $> n$ of $(r-1)n+1, (r-1)n+2, \dots, rn$, while x_1 ranges over all positive integers for which

$$\frac{a+\beta-1}{r+n} \leq \frac{R(g/x_1)}{g} < \frac{a}{r}, \frac{\beta}{n} \quad \left(a=1, \dots, \frac{r}{g}; \beta=1, \dots, \frac{n}{g} \right),$$

where g is the g. c. d. of r, n . Take $f(x) = 1$ or 0 according as x is an s th power or not. Then the functions

$$(1) \quad \sum_{k=1}^m f(k), \quad \sum_{y=1}^x \mu\left(\frac{x}{y}\right) f(y)$$

become $[\sqrt[s]{m}]$ and $\lambda_s(x)$, with the value 0 if the exponent of any prime factor of x is $\not\equiv 0, 1 \pmod{s}$, otherwise the value $(-1)^\sigma$, where σ is the number of primes occurring in x to the power $ks+1$. Thus

$$\begin{aligned} \sum_{x_1} \lambda_s(x_1) &= \left[\sqrt[s]{r+n} \right] - \left[\sqrt[s]{r} \right] - \left[\sqrt[s]{n} \right], \\ \sum_{x_2} \lambda_s(x_2) &= \left[\sqrt[s]{rn} \right] - \left[\sqrt[s]{(r-1)n} \right] - \left[\sqrt[s]{n} \right]. \end{aligned}$$

If $f(x) = 0$ or 1 according as x is divisible by an s th power or not, the functions (1) become $Q_s(m)$ and $\mu(\sqrt[s]{x})$, the former being the number of integers $\leq m$ divisible by no s th power. If $f(x) = 1$ or 0 according as x is prime or not, the functions (1) become the number of primes $\leq m$ and a simple function $\alpha(x)$; then the third formula shows that the mean density of the primes $\leq r$ is

$$\sum_{y=1}^r \alpha(y) \left\{ R\left(\frac{1}{y}\right) - \frac{1}{r} R\left(\frac{r}{y}\right) \right\}.$$

^{10a}Denkschr. Akad. Wien (Math.), 49, II, 1885, 108.

¹¹Sitzungsber. Akad. Wiss. Wien (Math.), 94, 1886, II, 714.

¹²*Ibid.*, 97, 1888, IIa, 420-6.

If $f(x) = \log x$, the second function (1) becomes $\nu(x)$, having the value* $\log p$ when x is a power of the prime p , otherwise the value 0. Besides the resulting formulas, others are found by taking $f(x) = \nu(x)$, Jacobi's symbol (Δ/x) in the theory of quadratic residues, and finally the number of representations of x by the system of quadratic forms of discriminant Δ .

L. Saint-Loup¹³ represented graphically the divisors of a number. Write the first 300 odd numbers in a horizontal line; the 300 following numbers are represented by points above the first, etc. Take any prime as 17 and mark all its multiples; we get a rectilinear distribution of these multiples, which are at the points of intersection of two sets of parallel lines.

J. Hacks¹⁴ proved that the number of integers $\leq m$ which are divisible by an n th power > 1 is

$$p_n(m) = \Sigma \left[\frac{m}{k_1^n} \right] - \Sigma \left[\frac{m}{k_1^n k_2^n} \right] + \Sigma \left[\frac{m}{k_1^n k_2^n k_3^n} \right] - \dots,$$

where the k 's range over the primes > 1 [Bougaief⁶]. Then $\psi_2(m) = m - p_2(m)$ is the number of integers $\leq m$ not divisible by a square > 1 , and

$$\psi_2(m) + \psi_2\left(\frac{m}{4}\right) + \psi_2\left(\frac{m}{9}\right) + \dots + \psi_2\left(\frac{m}{[\sqrt{m}]^2}\right) = m.$$

A like formula holds for $\psi_3 = m - p_3(m)$, using quotients of m by cubes.

L. Gegenbauer^{14a} found the mean of the sum of the reciprocals of the k th powers of those divisors of a term of an unlimited arithmetical progression which are r th powers; also the probability that a term be divisible by no r th power; and many such results.

L. Gegenbauer¹⁵ noted that the number of integers $1, \dots, n$ not divisible by a λ th power is

$$(2) \quad Q_\lambda(n) = \sum_{x=1}^{[n^{1/\lambda}]} \left[\frac{n}{x^\lambda} \right] \mu(x).$$

Ch. de la Vallée Poussin¹⁶ proved that, if x is divided by each positive number $ky + b \leq x$, the mean of the fractional parts of the quotients has for $x = \infty$ the limit $1 - C$; if x is divided by the primes $\leq x$, the mean of the fractional parts of the quotients has for $x = \infty$ the limit $1 - C$. Here C is Euler's constant.⁸

L. Gegenbauer¹⁷ proved, concerning Dirichlet's³ quotients Q of the remainders (found on dividing n by $1, 2, \dots, n$ in turn) by the corresponding divisors, that the number of Q 's between 0 and $1/3$ exceeds the number of Q 's between $2/3$ and 1 by approximately $0.179n$, and similar theorems.

*Cf. Bougaief¹⁶ of Ch. XIX.

¹³Comptes Rendus Paris, 107, 1888, 24; École Norm. Sup., 7, 1890, 89.

¹⁴Acta Math., 14, 1890-1, 329-336.

^{14a}Sitzungsber. Ak. Wien (Math.), 100, IIa, 1891, 1018-1053.

¹⁵Ibid., 100, 1891, IIa, 1054. Denkschr. Akad. Wien (Math.), 49 I, II, 1885; 50 I, 1885. Cf. Gegenbauer⁷⁰ of Ch. X.

¹⁶Annales de la soc. sc. Bruxelles, 22, 1898, 84-90.

¹⁷Sitzungsberichte Ak. Wiss. Wien (Math.), 110, 1901, IIa, 148-161.

He investigated the related problem of Dirichlet.⁴ Finally, he used as divisors all the s th powers $\leq n$ and found the ratio of the number of remainders less than half of the corresponding divisors to the number of the others.

L. E. Dickson^{17a} and H. S. Vandiver proved that $2^n > 2(n+1)(n'+1)\dots$, if $1, n, n', \dots$ are the divisors of an odd number $n > 3$.

R. Birkeland¹⁸ considered the sum s_q of the q th powers of the roots a_1, \dots, a_m of $z^m + A_1 z^{m-1} + \dots + A_m = 0$. If s_1, \dots, s_m are divisible by the power α^p of a prime α , then A_q is divisible by α^p unless q is divisible by α . If q is divisible by α , and α^{p_1} is the highest power of α dividing q , then A_q is divisible by α^{p-p_1} . Then $(n + \alpha a_1) \dots (n + \alpha a_m) - n^m$ is divisible by α^p . In particular, the product of m consecutive odd integers is of the form $1 + 2^t$ if m is divisible by 2^p .

E. Landau¹⁹ reproduced Poussin's¹⁶ proof of the final theorem and added a simplification. He then proved a theorem which includes as special cases the two of Poussin and the final one by Dirichlet³. Given an infinite class of positive numbers q without a finite limit point and such that the number of q 's $\leq x$ is asymptotic to $x/w(x)$, where $w(x)$ is a non-decreasing positive function having

$$\lim_{x \rightarrow \infty} \frac{w(2x)}{w(x)} = 1;$$

then if x is divided by all the q 's $\leq x$, the mean of the fractional parts of the quotients has for $x = \infty$ the limit $1 - C$.

St. Guzel²⁰ wrote $\delta(n)$ for the greatest odd divisor of n and proved in an elementary way the asymptotic formulas

$$\sum_{n=1}^{[x]} \delta(n) = \frac{x^2}{3} + O(x), \quad \sum_{n=1}^{[x]} \frac{\delta(n)}{n} = \frac{2}{3}x + O(1),$$

for O as in Pfeiffer⁹⁰, Ch. X.

A. Axer²¹ considered the $\chi^{\lambda, \nu}(n)$ decompositions of n into such a pair of factors that always the first factor is not divisible by a λ th power and the second factor not by a ν th power, $\lambda \geq 2, \nu \geq 2$. Then $\sum_{n=1}^x \chi^{\lambda, \nu}(n)$ is given asymptotically by a complicated formula involving the zeta function.

F. Rogel²² wrote $R_{\lambda, n}$ for the algebraic sum of the partial remainders $t - [t]$ in (2), with n replaced by z , and obtained

$$Q_{\lambda}(z) = zP_{\lambda, n} + R_{\lambda, n}, \quad P_{\lambda, n} = \prod_{\nu=2}^n \left(1 - \frac{1}{p_{\nu}^{\lambda}}\right),$$

where p_n is the n th prime and $p_n^{\lambda} \leq z < p_{n+1}^{\lambda}$. He gave relations between the values of $Q_{\lambda}(z)$ for various z 's and treated sums of such values, and tabulated the values of $Q_2(z)$ and $R_{2, n}$ for $z \leq 288$. He^{22a} gave many relations

^{17a}Amer. Math. Monthly, 10, 1903, 272; 11, 1904, 38-9.

¹⁸Archiv Math. og Natur., Kristiania, 26, 1904, No. 10.

¹⁹Bull. Acad. Roy. Belgique, 1911, 443-472.

²⁰Wiadomosci mat., Warsaw, 14, 1910, 171-180.

²¹Prace mat. fiz., 22, 1911, 73-99 (Polish), 99-102 (German). Review in Bull. des sc. math., (2), 38, II, 1914, 11-13.

²²Sitzungsber. Ak. Wiss. Wien (Math.), 121, IIa, 1912, 2419-52.

^{22a}*Ibid.*, 122, IIa, 1913, 669-700. See Rogel²⁴³ of Ch. XVIII.

between the $Q_x(z)$, relations involving the number $A(z)$ of primes $\leq z$, and relations involving both Q 's and A 's.

A. Rothe²³ called b a maximal divisor of a if no larger divisor of a contains b as a factor. Then a/b is called the index of b with respect to a . If also c is a maximal divisor of b , etc., $a, b, c, \dots, 1$ are said to form a series of composition of a . In all series of composition of a , the sets of indices are the same apart from order [a corollary of Jordan's theorem on finite groups applied to the case of a cyclic group of order a].

*Weitbrecht²⁴ noted tricks on the divisibility of numbers.

*E. Moschietti²⁵ discussed the product of the divisors of a number.

Each²⁶ of the consecutive numbers 242, 243, 244, 245 has a square factor > 1 ; likewise for the sets of three consecutive numbers beginning with 48 or 98 or 124.

C. Avery and N. Verson²⁷ noted that the consecutive numbers 1375, 1376, 1377 are divisible by $5^3, 2^3, 3^3$, respectively.

J. G. van derCorput²⁸ evaluated the sum of the n th powers of all integers, not divisible by a square > 1 , which are $\leq x$ and are formed of r prime factors of m .

GREATEST COMMON DIVISOR, LEAST COMMON MULTIPLE.

On the number of divisions in finding the g. c. d. of two integers, see Lamé¹¹ *et seq.* in Ch. XVII; also Binet³³ and Dupré³⁴.

V. A. Lebesgue³⁵ noted that the l. c. m. of a, \dots, k is $(p_1 p_3 p_5 \dots) / (p_2 p_4 p_6 \dots)$ if p_1 is the product of a, \dots, k , while p_2 is the product of their g. c. d.'s two at a time, and p_3 the product of their g. c. d.'s three at a time, etc. If a, b, c have no common divisor, there exist an infinitude of numbers $ax + b$ relatively prime to c .

V. Bouniakowsky³⁶ determined the g. c. d. N of all integers represented by a polynomial $f(x)$ with integral coefficients without a common factor. Since N divides the constant term of $f(x)$, it remains to find the highest power p^μ of a prime p which divides $f(x)$ identically, *i. e.*, for $x = 1, 2, \dots, p^\mu$. Divide $f(x)$ by $X_p = (x-1) \dots (x-p)$ and call the quotient Q and remainder R . Then must $R \equiv 0 \pmod{p^\mu}$ for $x = 1, \dots, p$, so that each coefficient of R is divisible by p^μ , and $\mu \leq \mu_1$, where p^{μ_1} is the highest power of p dividing the coefficients of R . If $\mu_1 = 1$, we have $\mu = 1$. Next, let $\mu_1 > 1$. Divide

²³Zeitschrift Math.-Naturw. Unterricht, 44, 1913, 317-320.

²⁴Vom Zahlenkunststück zur Zahlentheorie, Korrespondenz-Blatt d. Schulen Württembergs, Stuttgart, 20, 1913, 200-6.

²⁵Suppl. al Periodico di Mat., 17, 1914, 115-6.

²⁶Math. Quest. Educ. Times, 36, 1881, 48.

²⁷Math. Miscellany, Flushing, N. Y., 1, 1836, 370-1.

²⁸Nieuw Archief voor Wiskunde, (2), 12, 1918, 213-27.

²⁹Jour. de Math., (1), 6, 1841, 453.

³⁰Ibid., (1), 11, 1846, 41.

³¹Nouv. Ann. Math., 8, 1849, 350; Introduction à la théorie des nombres, 1862, 51-53; Exercices d'analyse numérique, 1859, 31-32, 118-9.

³²Mém. acad. sc. St. Pétersbourg, (6), sc. math. et phys. 6 (sc. math. phys. et nat. 8), 1857 305-329 (read 1854); extract in Bulletin, 13, 149.

Q by $(x-p-1)\dots(x-2p)$ and call the quotient Q' and remainder R' . Then must $X_p R' + X_{2p} Q' \equiv 0$ and hence $X_p R' \equiv 0 \pmod{p^\mu}$. Thus if μ_2 is the exponent of the highest power of p dividing the coefficients of R' , we have $\mu \leq \mu_2 + 1$. In general, if μ_k and λ_{k-1} are the exponents of the highest powers of p dividing the coefficients of the remainder $R^{(k-1)}$ and $X_{(k-1)p}$ identically, then $\mu \leq \mu_k + \lambda_{k-1}$. Finally, if $l = [m/p]$, $\mu \leq \lambda_l$. The extension to several variables is said to present difficulties. [For simpler methods, see Hensel⁴⁴ and Borel.⁴⁸] It is noted (p. 323) that

$$(x^p - x)^n, \quad (x^{p(p^n)} - 1)x^n$$

are identically divisible by p^n . It is conjectured (p. 328) that $f(x)/N$ represents an infinitude of primes when $f(x)$ is irreducible.

E. Cesàro³⁷ and J. J. Sylvester³⁸ proved that the probability that two numbers taken at random from $1, \dots, n$ be relatively prime is $6/\pi^2$ asymptotically.

L. Gegenbauer³⁹ gave 16 sums involving the g. c. d. of several integers and deduced 37 asymptotic theorems such as the fact that the square of the g. c. d. of four integers has the mean value $15/\pi^2$. He gave the mean of the k th power of the g. c. d. of r integers.

J. Neuberg^{39a} noted that, if two numbers be selected at random from $1, \dots, N$, the probability that their sum is prime to N is $k = \phi(N)$ or $k/(N-1)$ according as N is odd or even.

T. J. Stieltjes,⁴⁰ starting with a set of n integers, replaced two of them by their g. c. d. and l. c. m., repeated the same operation on the new set, etc. Finally, we get a set such that one number of every pair divides the other. Such a reduced set is unique. The l. c. m. of a, \dots, l can be expressed (pp. 14-16) as a product $a' \dots l'$ of relatively prime factors dividing a, \dots, l , respectively. The l. c. m. (or g. c. d.) of a, b, \dots, l equals the quotient of $P = ab \dots l$ by the g. c. d. (or l. c. m.) of $P/a, P/b, \dots, P/l$.

E. Lucas⁴¹ gave theorems on g. c. d. and l. c. m.

L. Gegenbauer^{41a} considered in connection with the theory of primes, the g. c. d. of r numbers with specified properties.

J. Hacks⁴² expressed the g. c. d. of m and n in the forms

$$2 \sum_{s=1}^{n-1} \left[\frac{sm}{n} \right] - mn + m + n, \quad 2 \sum_{s=1}^{[n/2]} \left[\frac{sm}{n} \right] + 2 \sum_{s=1}^{[m/2]} \left[\frac{sn}{m} \right] - 2 \left[\frac{m}{2} \right] \left[\frac{n}{2} \right] + \epsilon,$$

where $\epsilon = 0$ or 1 according as m, n are both or not both even.

J. Hammond⁴³ considered arbitrary functions f and F of p and a , such

³⁷Mathesis, 1, 1881, 184; Johns Hopkins Univ. Circ., 2, 1882-3, 85.

³⁸Johns Hopkins Univ. Circ., 2, 1883, 45; Comptes Rendus Paris, 96, 1883, 409; Coll. Papers, 3, 675; 4, 86.

³⁹Sitzungsberichte Ak. Wiss. Wien (Math.) 92, 1885, II, 1290-1306.

^{39a}Math. Quest. Educ. Times, 50, 1889, 113-4.

⁴⁰Sur la théorie des nombres, Annales de la fac. des sciences de Toulouse, 4, 1890, final paper.

⁴¹Théorie des nombres, 1891, 345-6; 369, exs. 4, 5.

^{41a}Monatshefte Math. Phys., 3, 1892, 319-335.

⁴²Acta Math., 17, 1893, 208.

⁴³Messenger Math. 24 1894-5 17-19.

that $f(p, 0) = 1$, $F(p, 0) = 0$, and any two integers $m = \Pi p^a$, $n = \Pi p^\beta$, where the p 's are distinct primes and, for any p , $a \geq 0$, $\beta \geq 0$. Set

$$\psi(m) = \Pi f(p, a), \quad \Phi = \Sigma F(p, a).$$

By the usual proof that mn equals the product of the g. c. d. M of m and n by their l. c. m. μ , we get

$$\psi(m)\psi(n) = \psi(M)\psi(\mu), \quad \Phi(m) + \Phi(n) = \Phi(M) + \Phi(\mu).$$

In particular, if m and n are relatively prime,

$$\psi(m)\psi(n) = \psi(mn), \quad \Phi(m) + \Phi(n) = \Phi(mn).$$

These hold if ψ is Euler's ϕ -function, the sum $\sigma(m)$ of the divisors of m or the number $\tau(m)$ of divisors of m ; also, if $\Phi(m)$ is the number of prime factors of m or the sum of the exponents a in $m = \Pi p^a$.

K. Hensel⁴⁴ proved that the g. c. d. of all numbers represented by a polynomial $F(u)$ of degree n with integral coefficients equals the g. c. d. of the values of $F(u)$ for any $n+1$ consecutive arguments. For a polynomial of degree n_1 in u_1 , n_2 in u_2 , . . . we have only to use n_1+1 consecutive values of u_1 , n_2+1 consecutive values of u_2 , etc.

F. Klein⁴⁵ discussed geometrically Euclid's g. c. d. process.

F. Mertens⁴⁶ calls a set of numbers primitive if their g. c. d. is unity. If $m \neq 0$, $k > 1$, and a_1, \dots, a_k, m is a primitive set, we can find integers x_1, \dots, x_k so that $a_1 + mx_1, \dots, a_k + mx_k$ is a primitive set. Let d be the g. c. d. of a_1, \dots, a_k and find δ, μ so that $d\delta + m\mu = 1$. Take integral solutions α of $a_1\alpha_1 + \dots + a_k\alpha_k = d$ and primitive solutions β_i not all zero of $a_1\beta_1 + \dots + a_k\beta_k = 0$. Then $\gamma_i = \beta_i + \delta\alpha_i$ ($i = 1, \dots, k$) is a primitive set. Determine integers ξ so that $\gamma_1\xi_1 + \dots + \gamma_k\xi_k = 1$ and set $x_i = \mu\xi_i$. Then $a_i + mx_i$ form a primitive set.

R. Dedekind⁴⁷ employed the g. c. d. d of a, b, c ; the g. c. d. $(b, c) = a_1$, $(c, a) = b_1$, $(a, b) = c_1$. Then $a' = a_1/d$, $b' = b_1/d$, $c' = c_1/d$ are relatively prime in pairs. Then $db'b'c'$ is the l. c. m. of b_1, c_1 , and hence is a divisor of a . Thus $a = db'b'c'a''$, $b = dc'a'b''$, $c = da'b'c''$. The 7 numbers a', \dots, a'', \dots, d are called the "Kerne" of a, b, c . The generalization from 3 to n numbers is given.

E. Borel⁴⁸ considered the highest power of a prime p which divides a polynomial $P(x, y, \dots)$ with integral coefficients for all integral values of x, y, \dots . If each exponent is less than p , we have only to find the highest power of p dividing all the coefficients. In the contrary case, reduce all exponents below p by use of $x^p = x + px_1$, $x_1^p = x_1 + px_2, \dots$ and proceed as above with the new polynomial in $x, x_1, x_2, \dots, y, y_1, \dots$. Then to find all arithmetical divisors of a polynomial P , take as p in turn each prime less than the highest exponent appearing in P .

L. Kronecker⁴⁹ found the number of pairs of integers i, k having t as their g. c. d., where $1 \leq i \leq m$, $1 \leq k \leq n$. The quotient of this number by

⁴⁴Jour. für Math., 116, 1896, 350-6.

⁴⁵Ausgewählte Kapitel der Zahlentheorie, I, 1896.

⁴⁶Sitzungsberichte Ak. Wiss. Wien (Math.), 106, 1897, II a, 132-3.

⁴⁷Ueber Zerlegungen von Zahlen durch d. grössten gemeinsamen Teiler, Braunschweig, 1897.

⁴⁸Bull. Sc. Math. Astr., (2), 24 I, 1900, 75-80. Cf. Borel and Drach¹⁸⁰ of Ch. III.

⁴⁹Vorlesungen über Zahlentheorie, I, 1901, 306-312.

mn is the mean. When m and n increase indefinitely, the mean becomes $6/(\pi^2 t^2)$. The case $t=1$ gives the probability that two arbitrarily chosen integers are relatively prime; the proof in Dirichlet's *Zahlentheorie* fails to establish the existence of the probability.

E. Dintzl⁵⁰ proved that the g. c. d. $\Delta(a, \dots, e)$ is a linear function of a, \dots, e , and reproduced the proof of Lebesgue's³⁵ formula as given in Merten's *Vorlesungen über Zahlentheorie* and by de Jough.⁵¹

A. Pichler,^{50a} given the l. c. m. or g. c. d. of two numbers and one of them, found values of the other number.

J. C. Kluyver⁵² constructed several functions z (involving infinite series or definite integrals) which for positive integral values of the two real variables equals their g. c. d. He gave to Stern's⁵³ function the somewhat different form

$$z = 2 \sum_{\mu=0}^{[x]} P\left(\frac{\mu y}{x}\right), \quad P(u) \equiv u - [u] - \frac{1}{2}.$$

W. Sierpinski⁵⁴ stated that the probability that two integers $\leq n$ are relatively prime is

$$\frac{1}{n^2} \sum_{k=1}^n \mu(k) \left[\frac{n}{k} \right]^2,$$

contrary to Bachmann, *Analyt. Zahlentheorie*, 1894, 430.

G. Darbi⁵⁵ noted that if $\alpha = (a, N)$ is the g. c. d. of a, N ,

$$(N, abc \dots) = \alpha \left(b, \frac{N}{\alpha} \right) \left(c, \frac{N}{\alpha(b, N/\alpha)} \right) \dots$$

and gave a method of finding the g. c. d. and l. c. m. of rational fractions without bringing them to a common denominator.

E. Gelin⁵⁶ noted that the product of n numbers equals ab , where a is the l. c. m. of their products r at a time, and b is the g. c. d. of their products $n-r$ at a time.

B. F. Yanney⁵⁷ considered the greatest common divisors D_1, D_2, \dots of a_1, \dots, a_n in sets of k , and their l. c. m.'s L_1, L_2, \dots . Then

$$\prod_{i=1}^b D_i L_i^{k-1} \geq (a_1 \dots a_n)^c \geq \prod_{i=1}^b D_i^{k-1} L_i, \quad b = \binom{n}{k}, \quad c = \binom{n-1}{k-1}.$$

The limits coincide if $k=2$. The products have a single term if $k=n$.

P. Bachmann⁵⁸ showed how to find the number N obtained by ridding a given number n of its multiple prime factors. Let d be the g. c. d. of n and $\phi(n)$. If $\delta = n/d$ occurs to the r th power, but not to the $(r+1)$ th power in n , set $n_1 = n/\delta^r$. From n_1 build δ_1 as before, etc. Then $N = \delta \delta_1 \delta_2 \dots$

⁵⁰*Zeitschrift für das Realschulwesen*, Wien, 27, 1902, 654-9, 722.

^{50a}*Ibid.*, 26, 1901, 331-8.

⁵¹*Nieuw Archief voor Wiskunde*, (2), 5, 1901, 262-7.

⁵²K. Ak. Wetenschappen Amsterdam, *Proceedings of the Section of Sciences*, 5, II 1903, 658-662. (*Versl. Ak. Wet.*, 11, 1903, 782-6.)

⁵³*Jour. für Math.*, 102, 1888, 9-19.

⁵⁴*Wiadomosci Mat.*, Warsaw, 11, 1907, 77-80.

⁵⁵*Giornale di Mat.*, 46, 1908, 20-30.

⁵⁶*Il Pitagora*, Palermo, 16, 1909-10, 26-27.

⁵⁷*Amer. Math. Monthly*, 19, 1912, 4-6.

⁵⁸*Archiv Math. Phys.*, (3), 19, 1912, 283-5.

Erroneous remarks⁵⁹ have been made on the g. c. d. of $2^x - 1$, $3^x - 1$.

M. Lecat⁶⁰ noted that, if a_{ij} is the l. c. m. of i and j , the determinant $[a_{ij}]$ was evaluated by L. Gegenbauer,⁶¹ who, however, used a law of multiplication of determinants valid only when the factors are both of odd class.

J. Barinaga^{61a} proved that, if δ is prime to $N = nk$, the sum of those terms of the progression $N, N + \delta, N + 2\delta, \dots$, which are between nk and $n(k + h\delta)$ and which have with $n = mp$ the g. c. d. p , is $\frac{1}{2}n\phi(n/p)(2k + h\delta)h$.

R. P. Willaert⁶² noted that, if $P(n)$ is a polynomial in n of degree p with integral coefficients, $f(n) = aA^{an} + P(n)$ is divisible by D for every integral value of n if and only if the difference $\Delta^k f(0)$ of the k th order is divisible by D for $k = 0, 1, \dots, p + 1$. Thus, if $p = 1$, the conditions are that $f(0)$, $f(1)$, $f(2)$ be divisible by D .

*H. Verhagen⁶³ gave theorems on the g. c. d. and l. c. m.

H. H. Mitchell⁶⁴ determined the number of pairs of residues a, b modulo λ whose g. c. d. is prime to λ , such that ka, kb is regarded as the same pair as a, b when k is prime to λ , and such that λ and $ax + by$ have a given g. c. d.

W. A. Wijthoff⁶⁵ compared the values of the sums

$$\sum_{m=1}^{ab} (-1)^{m-1} m^s F\{(m, a)\}, \quad \sum_{m=1}^{(ab-1)/2} m^s F\{(m, a)\}, \quad s = 1, 2,$$

where (m, a) is the g. c. d. of m, a , while F is any arithmetical function.

F. G. W. Brown and C. M. Ross⁶⁶ wrote l_1, l_2, \dots, l_n for the l. c. m. of the pairs $A_1, A_2; A_2, A_3; \dots; A_n, A_1$, and g_1, g_2, \dots, g_n for the g. c. d. of these pairs, respectively. If L, G are the l. c. m. and g. c. d. of A_1, A_2, \dots, A_n , then

$$g_1 g_2 \dots g_n = G^n, \quad \frac{l_1 l_2 \dots l_n}{g_1 g_2 \dots g_n} = \frac{L^2}{G^2}.$$

C. de Polignac⁶⁷ obtained for the g. c. d. (a, b) of a, b results like

$$(a\lambda, b\mu) = (a, b) \cdot (\lambda, \mu) \cdot \left(\frac{a}{(a, b)}, \frac{\mu}{(\lambda, \mu)} \right) \cdot \left(\frac{b}{(a, b)}, \frac{\lambda}{(\lambda, \mu)} \right).$$

Sylvester⁶⁸ and others considered the g. c. d. of D_n and D_{n+1} where D_n is the n -rowed determinant whose diagonal elements are 1, 3, 5, 7, \dots , and having 1, 2, 3, 4, \dots in the line parallel to that diagonal and just above it, and units in the parallel just below it, and zeros elsewhere.

On the g. c. d., see papers 33–88, 215–6, 223 of Ch. V, Cesàro⁶¹ of Ch. X, Cesàro^{8, 9} of Ch. XI, and Kronecker³⁰ of Ch. XIX.

⁵⁹L'intermédiaire des math., 20, 1913, 112, 183–4, 228; 21, 1914, 36–7.

⁶⁰Ibid., 21, 1914, 91–2.

⁶¹Sitzungs. Ak. Wiss. Wien (Math.), 101, 1892, II a, 425–494.

^{61a}Annaes Sc. Acad. Polyt. do Porto, 8, 1913, 248–253.

⁶²Mathesis, (4), 4, 1914, 57.

⁶³Nieuw Tijdschrift voor Wiskunde, 2, 1915, 143–9.

⁶⁴Annals of Math., (2), 18, 1917, 121–5.

⁶⁵Wiskundige Opgaven, 12, 1917, 249–251.

⁶⁶Math. Quest. and Solutions, 5, 1918, 17–18.

⁶⁷Nouv. Corresp. Math., 4, 1878, 181–3.

⁶⁸Math. Quest. Educ. Times, 36, 1881, 97–8; correction, 117–8.

CHAPTER XII.

CRITERIA FOR DIVISIBILITY BY A GIVEN NUMBER.

In the Talmud¹, $100a+b$ is stated to be divisible by 7 if $2a+b$ is divisible by 7.

Hippolytos^{1a}, in the third century, examined the remainder on the division of certain sums of digits by 7 or 9, but made no application to checking numerical computation.

Avicenna or Ibn Sînâ (980–1037) is said to have been the discoverer of the familiar rule for casting out of nines (cf. Fontès³⁹); but it seems to have been of Indian origin.^{1b}

Alkarkhi^{1c} (about 1015) tested by 9 and 11.

Ibn Mûsâ Alchwarizmî^{1d} (first quarter of the ninth century) tested by 9.

Leonardo Pisano^{1e} gave in his *Liber Abbaci*, 1202, a proof of the test for 9, and indicated tests for 7, 11.

Ibn Albannâ^{1f} (born about 1252), an Arab, gave tests for 7, 8, 9.

In the fifteenth century, the Arab Sibte el-Mâridini^{1c} tested addition by casting out multiples of 7 or 8.

Nicolas Chuquet^{1g} in 1484 checked the four operations by casting out 9's.

J. Widmann^{1h} tested by 7 and 9.

Luca Paciolo² tested by 7, as well as by 9, the fundamental operations, but gave no rule to calculate rapidly the remainder on division by 7.

Petrus Apianus^{2a} tested by 6, 7, 8, 9.

Robert Recorde^{2b} tested by 9.

Pierre Forcadet³ noted that to test by $7=10-3$ we multiply the first digit by 3, subtract multiples of 7, add the residue to the next digit, then multiply the sum by 3, etc.

Blaise Pascal⁴ stated and proved a criterion for the divisibility of any number N by any number A . Let r_1, r_2, r_3, \dots , be the remainders obtained when $10, 10r_1, 10r_2, \dots$ are divided by A . Then $N = a + 10b + 100c + \dots$ is divisible by A if and only if $a + r_1b + r_2c + \dots$ is divisible by A .

¹Babylonian Talmud, Wilna edition by Romm, Book Aboda Sara, p. 9b.

^{1a}M. Cantor, *Geschichte der Math.*, ed. 3, I, 1907, 461.

^{1b}*Ibid.*, 511, 611, 756–7, 763–6.

^{1c}Cf. Carra de Vaux, *Bibliotheca Math.*, (2), 13, 1899, 33–4.

^{1d}M. Cantor, *Geschichte der Math.*, ed. 3, I, 1907, 717.

^{1e}Scritti, 1, 1857, 8, 20, 39, 45; Cantor, *Geschichte*, 2, 1892, 8–10.

^{1f}Le Talkhys d'Ibn Albannâ publié et traduit par A. Marre, *Atti Accad. Pont. Nuovi Lincei*, 17, 1863–4, 297. Cf. M. Cantor, *Geschichte Math.*, I, ed. 2, 757, 759; ed. 3, 805–8.

^{1g}Le Triparty en la science de nombres, *Bull. Bibl. St. Sc. Math.*, 13, 1880, 602–3.

^{1h}Behêde vnd hubsche Rechnung. . . , Leipzig, 1489.

²Summa de arithmetica geometria proportioni et proportionalita, Venice, 1494, f. 22, r.

^{2a}Ein neue. . . Kauffmans Rechnung, Ingolstadt, 1527, etc.

^{2b}The Grovnd of Artes, London, c. 1542, etc.

³L'Arithmétique de P. Forcadet de Beziers, Paris, 1556, 59–60.

⁴De numeris multiplicibus, presented to the Académie Parisienne, in 1654, first published in 1665; *Oeuvres de Pascal*, 3, Paris, 1908, 311–339; 5, 1779, 123–134.

D'Alembert⁶ noted that if $N = A \cdot 10^m + B \cdot 10^n + \dots + E$ is divisible by $10 - b$, then $Ab^m + Bb^n + \dots + E$ is divisible by $10 - b$; if N is divisible by $10 + b$, then $A(-b)^m + B(-b)^n + \dots + E$ is divisible by $10 + b$. The case $b = 1$ gives the test for divisibility by 9 or 11. By separating N into parts each with an even number of digits, $N = A \cdot 10^m + \dots + E$, where m, \dots are even; then if N is divisible by $100 - b$, $Ab^{m/2} + \dots + E$ is divisible by $100 - b$.

De Fontenelle⁶ gave a test for divisibility by 7 which is equivalent to the case $b = 3$ of D'Alembert; to test 3976 multiply the first digit by 3 and add to the second digit; it remains to test 1876. For proof see F. Sanvitali, *Hist. Literariae Italiae*, vol. 6, and Castelvetri.⁸

G. W. Kraft⁷ gave the same test as Pascal for the factor 7.

J. A. A. Castelvetri⁸ gave the test for 99: Separate the digits in pairs, add the two-digit components, and see if the sum is a multiple of 99. For 999 use triples of digits.

Castelvetri⁹ tested 1375, for example, for the factor 11 by noting that $13 + 75 = 88$ is divisible by 11. If the resulting sum be composed of more than two digits, pair them, add and repeat. To test for the factor 111, separate the digits into triples and add. The proof follows from the fact that 10^{2k} has the remainder 1 when divided by 11.

J. L. Lagrange¹⁰ modified the method of Pascal by using the least residue modulo A (between $-A/2$ and $A/2$) in place of the positive residue. He noted that if a number is written to any base a its remainder on division by $a - 1$ is the same as for the sum of its digits.

J. D. Gergonne¹¹ noted that on dividing $N = A_0 + A_1b^m + A_2b^{2m} + \dots$, written to base b , by a divisor of $b^m - 1$, the remainder is the same as on dividing the sum $A_0 + A_1 + A_2 + \dots$ of its sets of m digits. Similarly for $b^m + 1$ and $A_0 - A_1 + A_2 - A_3 + \dots$.

C. J. D. Hill¹² gave rules for abbreviating the testing for a prime factor p , for $p < 300$ and certain larger primes.

C. F. Liljevalch^{12a} noted that if $10^na - \beta$ is divisible by p then $a - 10^nb$ will be a multiple of p if and only if $aa - \beta b$ is a multiple of p .

J. M. Argardh¹³ used Hill's symbols, treating divisors 7, 17, 27, 1429.

F. D. Herter¹⁴ noted that $a + 10b + 100c + \dots$ is divisible by $10n \pm 1$ if

⁶Manuscript R. 240* 6 (8°), Bibl. Inst. France, 21, ff. 316-330, Sur une propriété des nombres.

⁶Histoire Acad. Paris, année 1728, 51-3.

⁷Comm. Ac. Sc. Petrop, 7, ad annos 1734-5, p. 41.

⁸De Bononiensi Scientiarum et Artium Instituto atque Academia Comm., 4, 1757; commentarii, 113-139; opuscula, 242-260.

⁹De Bononiensi Scientiarum et Artium Instituto atque Academia Comm., vol. 5, 1767, part 1, pp. 134-144; part 2, 108-119.

¹⁰Leçons élém. sur les math. données à l'école normale en 1795, Jour. de l'école polytechnique, vols. 7, 8, 1812, 194-9; Oeuvres, 7, pp. 203-8.

¹¹Annales de math. (ed., Gergonne), 5, 1814-5, 170-2.

¹²Jour. für Math., 11, 1834, 251-261; 12, 1834, 355. Also, De factoribus numerorum compositorum dignoscendis, Lund, 1838.

^{12a}De factoribus numerorum compositorum dignoscendis, Lund, 1838.

¹³De residuis ex divisione . . . , Diss. Lund, 1839.

¹⁴Ueber die Kennzeichen der Theiler einer Zahl, Progr. Berlin, 1844.

$a \mp b/n + c/n^2 \mp \dots$ is divisible by $10n \pm 1$, with a like test for $10n \pm 3$ (replacing $1/n$ by $3/n$), and deduced the usual tests for 9, 11, 7, 13, etc.

A. L. Crelle¹⁵ noted that to test $x_m A^m + \dots + x_1 A + x_0$ for the divisor s we may select any integer n prime to s , take $r \equiv nA \pmod{s}$, and test

$$x_m r^m + n x_{m-1} r^{m-1} + \dots + n^m x_0$$

for the divisor s . For example, if $A = 10$, $s = 7$, $10^3 \equiv -1 \pmod{7}$, so that $x_0 - x_1 + x_2 - \dots \pm x_m$ is to be tested for the divisor 7, where x_0, \dots are the three-digit components of the proposed number from right to left. Similarly for $s = 9, 11, 13, 17, 19$.

A. Transon¹⁶ gave a test for the divisibility of a number by any divisor of $10^a \cdot n \pm 1$.

A. Niegemann¹⁷ noted that 354578385 is divisible by 7 since $35457 + 2 \times 8385$ is divisible by 7. In general if the number formed by the last m digits of N is multiplied by k , and the product is added to the number derived from N by suppressing those digits, then N is divisible by d if the resulting sum is divisible by d . Here $k(0 < k < d)$ is chosen so that $10^m k - 1$ is divisible by d . Thus $k = 2$ if $m = 4$, $d = 7$.

Many of the subsequent papers are listed at the end of the chapter.

H. Wilbraham¹⁸ considered the exponent p to which 10 belongs modulo m , where m is not divisible by 2 or 5. Then the decimal for $1/m$ has a period of p digits. If any number N be marked off into periods of p digits each, beginning with units, so that $N = a_1 + 10^p a_2 + 10^{2p} a_3 + \dots$, then $a_1 + a_2 + \dots \equiv N \pmod{m}$, and N is divisible by m if and only if $a_1 + a_2 + \dots$ is divisible by m .

E. B. Elliott¹⁹ let $10^p = MD + r_p$. Thus $N = 10^p n_p + \dots + 10n_1 + n_0$ is divisible by D if $N = \sum n_j MD + \sum n_j r_j$ is divisible by D . The values of the r 's are tabulated for $D = 3, 7, 8, 9, 11, 13, 17$.

A. Zbikowski²⁰ noted that $N = a + 10k$ is divisible by 7 if $k - 2a$ is divisible by 7. If δ is of the form $10n + 1$, $N = a + 10k$ is divisible by δ if $k - na$ is divisible by δ ; this holds also if δ is replaced by a divisor of a number $10n + 1$.

V. Zeipel²¹ tests for a divisor b by use of $nb = 10d + 1$. Then $10a_2 + a_1$ is divisible by b if $a_2 - a_1 d$ is divisible by b .

J. C. Dupain²² noted, for use when division by $p - 1$ is easy, that $N = (p - 1)Q + R$ is divisible by p if $R - Q$ is divisible by p .

F. Folie²³ proved that if a, c are such that $ak' \pm ck = mp$ then $AB + C$ is divisible by the prime $p = aB + c$ if $Ak' \pm Ck = m'p$, provided a, c, k, k' are

¹⁵Jour. für Math., 27, 1844, 125-136.

¹⁶Nouv. Ann. Math., 4, 1845, 173-4 (cf. 81-82 by O. R.).

¹⁷Entwicklung u. Begründung neuer Gesetze über die Theilbarkeit der Zahlen. Jahresber. Kath. Gym. Köln, 1847-8.

¹⁸Cambridge and Dublin Math. Jour., 6, 1851, 32.

¹⁹The Math. Monthly (ed. Runkle), 1, 1859, 45-49.

²⁰Bull. ac. sc. St. Pétersbourg, (3), 3, 1861, 151-3; Mélanges math. astr. ac. St. Pétersbourg, 3, 1859-66, 312.

²¹Öfversigt finska vetensk. förhandl., Stockholm, 18, 1861, 425-432.

²²Nouv. Ann. Math., (2), 6, 1867, 368-9.

²³Mém. Soc. Sc. Liège, (2), 3, 1873, 85-96.

not multiples of p . Application is made to the primes $p \leq 37$. Again, if p is a prime and

$$aB^2 + cB + d = ak'' + ck' + dk = Ak'' + Ck' + Dk = mp,$$

where k, k', k'' are prime to p , then $AB^2 + CB + D$ is divisible by p provided $k'^2 - kk''$ is a multiple of p .

C. F. Möller and C. Holten²⁴ would test the divisibility of n by a given prime p by seeking a such that $ap \equiv \pm 1 \pmod{10}$ and subtracting from n such a multiple of ap that the difference ends with zero.

L. L. Hommel²⁵ made remarks on the preceding method.

V. Schlegel²⁶ noted that if the divisor to be tested ends with 1, 3, 7 or 9, its product by 1, 7, 3 or 9 is of the form $d = 10\lambda + 1$. Then a , with the final digit u , is divisible by d if $a_1 = (a - ud)/10$ is. Then treat a_1 as we did a , etc.

P. Otto²⁷ would test Z for a given prime factor p by seeking a number n such that if the product by n of the number formed by the last s digits of Z be subtracted from the number represented by the remaining digits, the remainder is divisible by p if and only if Z is. Material is tabulated for the application of the method when $p < 100$.

N. V. Bougaief^{27a} noted that $a_\mu \dots a_1$ to base B is divisible by D if $a_1 \dots a_\mu$ to base d is divisible by D , where $dB \equiv 1 \pmod{D}$. For $B = 10$ and $D = 10n + 9, 1, 3, 7$, we may take $d = n + 1, 9n + 1, 3n + 1, 7n + 5$, respectively. Again, $kB^2 + aB + b$ is divisible by D if $kB + a + bd$ is divisible.

W. Mantel and G. A. Oskamp²⁸ proved that, to test the divisibility of a number to any base by a prime, the value of the coefficient required to eliminate one, two, . . . digits on subtraction is periodic. Also the number of terms of the period equals the length of the period of the periodic fraction arising on division by the same prime.

G. Dostor^{28a} noted that $10t + u$ is divisible by any divisor a of $10A \equiv 1$ if $t \equiv Au$ is divisible by a . [A case of Liljevalch^{12a}.]

Hočevar²⁹ noted that if N , written to base a , is separated into groups G_1, G_2, \dots each of q digits, N is divisible by a factor of $a^q + 1$ if $G_1 - G_2 + G_3 - \dots$ is divisible. Thus, for $a = 2, q = 4, N = 104533$, or 11001100001010101 to base 2 is divisible by 17 since $0101 - 0101 + 1000 - 1001 + 1 = 0$.

J. Delboeuf³⁰ stated that if p, q are such that $pa + qb$ is a multiple of D and if $N = Aa + B\beta$ is a multiple of $D = aa + b\beta$, then $pA + qB$ is a multiple of D .

E. Catalan (*ibid.*, p. 508) stated and proved the preceding test in the following form: If a, b and also a', b' are relatively prime, and

$$N = aa' + bb', \quad Nx = Aa + Bb, \quad Nx' = A'a' + B'b',$$

then $AA' + BB'$ is a multiple of N (and a sum of 2 squares if N is).

²⁴Tidsskrift for Math., (3), 5, 1875, 177-180.

²⁵Tidsskrift for Math., (3), 6, 1876, 15-19.

²⁶Zeitschrift Math. Phys., 21, 1876, 365-6.

²⁷Zeitschrift Math. Phys., 21, 1876, 366-370.

^{27a}Mat. Sbornik (Math. Soc. Moscow), 8, 1876, I, 501-5.

²⁸Nieuw Archief voor Wiskunde, Amsterdam, 4, 1878, 57-9, 83-94.

^{28a}Archiv Math. Phys., 63, 1879, 221-4.

²⁹Zur Lehre von der Teilbarkeit . . . , Prog. Innsbruck, 1881.

³⁰La Revue Scientifique de France, (3), 38, 1886, 377-8.

Noël (*ibid.*, 378-9) gave tests for divisors 11, 13, 17, . . . , 43.

Bougon (*ibid.*, 508) gave several tests for the divisor 7. For example, a number is divisible by 7 if the quadruple of the number of its tens diminished by the units digit is divisible by 7, as 1883 since $188 \cdot 4 - 3 = 749$ is divisible by 7. J. Heilmann (*ibid.*, 187) gave a test for the divisor 7.

P. Breton and Schobbens (*ibid.*, 444-5) gave tests for the divisor 13.

S. Dickstein³¹ gave a rule to reduce the question of the divisibility of a number to any base by another to that for a smaller number.

A. Loir³² gave a rule to test the divisibility of N , having the units digit a , by a prime P . From $(N-a)/10$, subtract the product of a by the number, say $(mP-1)/10$, of tens in such a multiple mP of P that the units digit is 1. To the difference obtained apply the same operation, etc., until we exhaust N . If the final difference be P or 0, N is divisible by P .

R. Tucker³³ started with a number N , say 5443, cut off the last digit 3 and defined $u_2 = 544 - 2 \cdot 3 = 538$, $u_3 = 53 - 2 \cdot 8$, etc. If any one of the u 's is divisible by 7, N is divisible by 7. R. W. D. Christie (p. 247) extended the test to the divisors 11, 13, 17, 37, the respective multipliers being 1, 9, 5, 11, provided always the number tested ends with 1, 3, 7 or 9.

R. Perrin³⁴ would find the minimum residue of N modulo p as follows. Decompose N , written to base x , into any series of digits, each with any number of digits, say A, B_i, C_j, \dots , where B_i has i digits. Let p be any integer prime to x and find q_1 so that $q_1 x \equiv 1 \pmod{p}$. Let a be any one of the integers prime to p and numerically $< p/2$. Let β be the i th integer following a in that one of the series containing a which are defined thus: as the first series take the residues modulo p of $1, q, q^2, \dots$; as the second series take the products of the preceding residues by any new integer prime to p ; etc. Let γ be the j th integer following β in the same series, etc. Then $N' = Aa + B_i\beta + C_j\gamma + \dots$ is or is not divisible by p according as N is or not. By repetitions of the process, we get the minimum residue of N modulo p . The special case $A + B_1q_1$, with p a prime, is due to Loir.³²

Dietrichkeit³⁵ would test $Z = 10k + a$ for the divisor n by testing $k - xa$, where $10x + 1$ is some multiple of n . To test Z (pp. 316-7) for the divisor 7, test the sum of the products of the units digit, tens digit, . . . by 1, 3, 2, 6, 4, 5, taken in cyclic order beginning with any term (the remainders on converting $1/7$ into a decimal fraction). Similarly for $1/n$, when n is prime to 10.

J. Fontès³⁶ would test N for a divisor M by using a number $< N$ and $\equiv N \pmod{M}$, found as follows. For the base B , let q be the absolutely least residue of B^m modulo M . Commencing at the right, decompose N into sets of m digits, as λ_m, \dots, a_m , and set $f(x) = a_m x^n + \beta_m x^{n-1} + \dots + \lambda_m$, whence $N = f(B^m)$. By expanding $N = f(q + M\Omega)$, we see that $f(q)$ is the desired number $< N$ and $\equiv N \pmod{M}$.

S. Levänen³⁷ gave a table showing the exponent to which 10 belongs for

³¹Lemberg Museum (Polish), 1886. ³²Comptes Rendus Paris, 106, 1888, 1070-1; errata, 1194.

³³Nature, 40, 1889, 115-6.

³⁴Assoc. franç. avanc. sc., 18, 1889, II, 24-38.

³⁵Zeitschr. Math. Phys., 36, 1891, 64.

³⁶Comptes Rendus Paris, 115, 1892, 1259-61.

³⁷Öfversigt af finska vetenskaps-soc. förhandlingar, 34, 1892, 109-162. Cf. Jahrbuch Fortschr. Math., 24, 1892, 164-5.

primes $b < 200$ and certain larger primes, from which are easily deduced tests for the divisor b .

Several^{37a} noted that if 10 belongs to the exponent n modulo d , and if S_1, S_2, \dots denote the sums of every n th digit of N beginning with the first, second, . . . at the right, the remainder on the division of N by d is that of $S_1 + 10S_2 + 10^2S_3 + \dots$.

J. Fontès³⁸ would find the least residue of N modulo M . If 10^n has the residue q modulo M , we do not change the least residue of N if we multiply a set of n digits of N by the same power of q as of 10^n . Thus for $M = 19$, $N = 10433 = 10^4 + 4 \cdot 10^2 + 33$, 10^2 has the residue 5 modulo 19 and we may replace N by $5^2 + 4 \cdot 5 + 33$. The method is applied to each prime $M \leq 149$.

Fontès³⁹ gave a history of the tests for divisibility, and an "extension of the method of Pascal," similar to that in his preceding paper.

P. Valerio⁴⁰ would test the divisibility of N by 39, for example, by subtracting from N a multiple of 39 with the same ending as N .

F. Bělohlávek⁴¹ noted that $10A + B$ is divisible by $10p \pm 1$ if $A \mp pB$ is.

C. Börgen⁴² noted that $Z = a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0$ is divisible by N if

$$\sum_{\nu=0}^{n-a+1} (a_{\nu-a+1} \cdot 10^{a-1} + \dots + a_\nu)(10^a - N)^{\nu/a}$$

is divisible by N . For $N = 7$, take $a = 1$; then $10^a - N = 3$ and Z is divisible by 7 if $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \dots$ is divisible by 7.

J. J. Sylvester^{42a} noted that, if the r digits of N , read from left to right, be multiplied by the first r terms of the recurring series 1, 4, 3, -1, -4, -3; 1, 4, . . . [the residues, in reverse order, of 10, $10^2, \dots$, modulo 13], the sum of the products is divisible by 13 if and only if N is divisible by 13.

C. L. Dodgson^{42b} discussed the quotient and remainder on division by 9 or 11.

L. T. Riess⁴³ noted that, if p is not divisible by 2 or 5, $10b + a$ ($a < 10$) is divisible by p if $b - xa$ is divisible by p , where $mp = 10x + a$ ($a < 10$) and $m = 1, 7, 3, 9$ according as $p \equiv 1, 3, 7, 9 \pmod{10}$, respectively.

A. Loir⁴⁴ gave tests for prime divisors < 100 by uniting them by twos or threes so that the product P ends in 01, as $7 \cdot 43 = 301$. To test N , multiply the number formed of the last two digits of N by the number preceding 01 in P , subtract the product from N , and proceed in the same manner with the difference. Then P is a factor if we finally get a difference which is zero. If a difference is a multiple of a prime factor p of P , then N is divisible by p .

Plakhowo⁴⁵ gave the test by Bougaief, but without using congruences.

^{37a}Math. Quest. Educ. Times, 57, 1892, 111.

³⁸Assoc. franç. avanc. sc., 22, 1893, II, 240-254.

³⁹Mém. ac. sc. Toulouse, (9), 5, 1893, 459-475.

⁴⁰La Revue Scientifique de France, (3), 52, 1893, 765.

⁴¹Casopis, Prag, 23, 1894, 59.

⁴²Nature, 57, 1897-8, 54.

^{42a}Educat. Times, March, 1897. Proofs, Math. Quest. Educ. Times, 66, 1897, 108. Cf. W. E.

Heal, Amer. Math. Monthly, 4, 1897, 171-2.

^{42b}Nature, 56, 1897, 565-6.

⁴³Russ. Nat., 1898, 329. Cf. Jahrb. Fortschritte Math., 29, 1898, 137.

⁴⁴Assoc. franç. avanc. sc., 27, 1898, II, 144-6.

⁴⁵Bull. des sc. math. et phys. élémentaires, 4, 1898-9, 241-3.

To test $N = a_0 + a_1B + \dots + a_nB^n$ for the divisor D prime to B , determine d and x so that $Bd = Dx + 1$. Multiply this equation by a_0 and subtract from N . Thus

$$N = BN' - Da_0x, \quad N' = a_0d + (a_1 + a_2B + \dots + a_nB^{n-1})B.$$

Hence N is divisible by D if and only if N' is divisible by D . Now, N' is derived from N by supressing the units digit a_0 and adding to the result the product a_0d . Next operate with N' as we did with N .

J. Malengreau⁴⁶ would test N for a factor q prime to 10 by seeking a multiple $11\dots 1$ (to m digits) of q , then an exponent t such that the number of digits of $10^t N$ is a multiple of m . From each set of m digits of $10^t N$ subtract the nearest multiple of $1\dots 1$ (to m digits). The sum of the residues is divisible by q if and only if N is divisible by q .

G. Loria⁴⁷ proved that $N = a_0 + ga_1 + \dots + g^k a_k$ is divisible by a if and only if a divides the sum $a_0 + \dots + a_k$ of the digits of N written to a base g of the form $ka + 1$; or if a divides $a_0 - a_1 + a_2 - \dots$ when the base g is of the form $ka - 1$. Taking $g = 10^m$, we have the test, in Gelin's *Arithmétique*, in terms of groups of m digits. We may select m to be $\frac{1}{2}\phi(a)$ or a number such that $10^m \equiv \pm 1$ has the factor a . In place of $a_0 + a_1 + \dots$ when $g = 10^m$, we may employ

$$\rho a_0 + \lambda a_1 + 10\lambda a_2 + \dots + 10^{m-2}\lambda a_{m-1} \\ + \sum_{k=1}^{n-1} 10^{km-1}\lambda(a_{km} + 10a_{km+1} + \dots + 10^{m-1}a_{km+m-1}),$$

where $\lambda = 1, 2$ or 5 , and ρ is determined by $10\rho/\lambda \equiv 1 \pmod{a}$. Taking $a = 7, 13, 17, 19, 23$, special tests for divisors are obtained.

G. Loria⁴⁸ proved that, if a_0, a_1, \dots are successive sets of t digits of N , counted from the right, and $\sigma = a_0 \pm a_1 + a_2 \pm a_3 + \dots$, then

$$N - \sigma = a_1(10^t \mp 1) + a_2(10^{2t} - 1) + a_3(10^{3t} \mp 1) + \dots,$$

so that a factor of $10^t \mp 1$ divides N if and only if it divides σ .

A. Tagiuri⁴⁹ extended the last result to any base g . We have

$$N = a_0 + ga_1 + \dots = N_{0m} + g^m N_{1m} + g^{2m} N_{2m} + \dots$$

if $N_{\rho m} = a_{\rho m} + a_{\rho m+1}g + \dots + a_{\rho m+m-1}g^{m-1}$. Hence, if $g^m \equiv \pm 1 \pmod{a}$,

$$N \equiv N_{0m} \pm N_{1m} + N_{2m} \pm \dots \pmod{a}.$$

L. Ripert⁵⁰ noted that $10D + u$ is divisible by $10\delta + i$ if $Di - \delta u$ is divisible, and gave many tests for small divisors.

G. Biase⁵¹ derived tests that $10d + u$ has the factor 7 or 19 from

$$2(10d + u) \equiv 2u - d \pmod{7}, \quad 2(10d + u) \equiv 2u + d \pmod{19}.$$

O. Meissner⁵² reported on certain tests cited above.

⁴⁶Mathesis, (3), 1, 1901, 197-8.

⁴⁷Rendiconti Accad. Lincei (Math.), (5), 10, 1901, sem. 2, 150-8. Mathesis, (3), 2, 1902, 33-39.

⁴⁸Il Boll. Matematica Gior. Sc.-Didat., Bologna, 1, 1902. Cf. A. Bindoni, *ibid.*, 4, 1905, 87.

⁴⁹Periodico di Mat., 18, 1903, 43-45.

⁵⁰L'enseignement math., 6, 1904, 40-46.

⁵¹Il Boll. Matematica Gior. Sc.-Didat., Bologna, 4, 1905, 92-6.

⁵²Math. Naturw. Blätter, 3, 1906, 97-99.

E. Nannei⁵³ employed $r_1 = a_1 - a_0x$, $r_2 = a_2 - r_1x, \dots$ ($x < 10$). Then, if $r_n = 0$, $N = 10^n a_n + \dots + 10a_1 + a_0$ is divisible by $10x + 1$ and the quotient has the digits $r_{n-1}, r_{n-2}, \dots, r_1, a_0$. The cases $x = 1, 2$ are discussed and several tests for 7 deduced. For $x = 1/3$, we conclude that, if $r_n = 0$, N is divisible by 13 and the digits of the quotient are $r_{n-1}/3, \dots, r_1/3, a_0/3$.

A. Chiari⁵⁴ employed D'Alembert's⁵ method for $10 + b$, $b = 3, 7, 9$.

G. Bruzzone⁵⁵ noted that, to find the remainder R when N is divided by an integer x of r digits, we may choose y such that $x + y = 10^r$, form the groups of r digits counting from the right of N , and multiply the successive groups (from the right) by $1, y, y^2, \dots$ or by their residues modulo x ; then R equals the remainder on dividing the sum of the products by x . If we choose $x - y = 10^r$, we must change alternate signs before adding. For practical use, take $y = 1$.

Fr. Schuh⁵⁶ gave three methods to determine the residue of large numbers for a given modulus.

Stuyvaert⁵⁷ let a, b, \dots be the successive sets of n digits of N to the base B , so that $N = a + bB^n + cB^{2n} + \dots$. Then N is divisible by a factor D of $B^n \mp R^n$ if and only if $a \pm bR^n + cR^{2n} \pm \dots$ is divisible by D . For $R = 1$, $B = 10$, $n = 1, 2, \dots$, we obtain tests for divisors of 9, 99, 11, 101, etc. A divisor, prime to B , of $mB + 1$ divides $N = a + bB$ if and only if it divides $b - ma$.

FURTHER PAPERS GIVING TESTS FOR A GIVEN DIVISOR d .

J. R. Young and Mason for $d = 7, 13$ [Pascal⁴], Ladies' Diary, 1831, 34-5, Quest. 1512.

P. Gorini [Pascal⁴], Annali di Fis., Chim. Mat., (ed., Majocchi), 1, 1841, 237.

A. Pinaud for $d = 7, 13$, Mém. Acad. Sc. Toulouse, 1, 1844, 341, 347.

*Dietz and Vincenot, Mém. Acad. Metz, 33, 1851-2, 37.

Anonymous writer for $d = 9, 11$, Jour. für Math., 50, 1855, 187-8.

*H. Wronski, Principes de la phil. des math. Cf. de Montferrier, Encyclopédie math., 2, 1856, p. 95.

O. Terquem for $d \leq 19, 23, 37, 101$, Nouv. Ann. Math., 14, 1855, 118-120.

A. P. Reyer for $d = 7$, Archiv Math. Phys., 25, 1855, 176-196.

C. F. Lindman for $d = 7, 13$, *ibid.*, 26, 1856, 467-470.

P. Buttel for $d = 7, 9, 11, 17, 19$, *ibid.*, 241-266.

De Lapparent [Herter¹⁴], Mém. soc. imp. sc. nat. Cherbourg, 4, 1856, 235-258.

Karwowski [Pascal⁴], Ueber die Theilbarkeit..., II, Progr., Lissa, 1856.

*D. van Langeraad, Kenmerken van deelbaarheid der geheele getallen, Schoonhoven, 1857.

Flohr, Ueber Theilbarkeit und Reste der Zahlen, Progr., Berlin, 1858.

V. Bouniakowsky for $d = 37, 989$, Nouv. Ann. Math., 18, 1859, 168.

Elefanti for $d = 7 \cdot 13$, Proc. Roy. Soc. London, 10, 1859-60, 208.

A. Niegemann for $d = 10^m \cdot n + a$, Archiv Math. Phys., 38, 1862, 384-8.

J. A. Grunert for $d = 7, 11, 13$, *ibid.*, 42, 1864, 478-482.

V. A. Lebesgue, Tables diverses pour la décomposition des nombres, Paris, 1864, p. 13.

⁵³Il Pitagora, Palermo, 13, 1906-7, 54-9.

⁵⁴*Ibid.*, 14, 1907-8, 35-7.

⁵⁵*Ibid.*, 15, 1908-9, 119-123.

⁵⁶Supplém. De Vriend der Wiskunde, 24, 1912, 89-103.

⁵⁷Les Nombres Positifs, Gand, 1912, 59-62.

- C. M. Ingleby for $d=9, 11$, British Assoc. Report, 35, 1865, 7 (trans.).
M. Jenkins for any prime d , Math. Quest. Educ. Times, 8, 1868, 69, 111.
F. Unferdinger [Gergonne¹¹], Sitzungsber. Ak. Wiss. Wien (Math.), 59, 1869, II, 465-6.
H. Anton for $d=9, 11, 13, 101$, Archiv Math. Phys., 49, 1869, 241-308.
W. H. Walenn, British Assoc. Report, 40, 1870, 16-17 (trans.); Phil. Mag., (4), 36, 1868, 346-8; (4), 46, 1873, 36-41; (4), 49, 1875, 346-351; (5), 2, 1876, 345; 4, 1877, 378; 9, 1880, 56, 121, 271.
M. A. X. Stouff for $d < 100$, Nouv. Ann. Math., (2), 10, 1871, 104.
J. Lubin, *ibid.*, (2), 12, 1874, 528-30 (trivial).
Szenic for $d=7, 9, 37$, Von der Kongruenz der Z., Progr. Schrimm, 1873.
E. Brooks for $d=7$, Des Moines Analyst, 2, 1875, 129.
W. J. Greenfield and M. Collins for $d=47, 73$, Math. Quest. Educ. Times, 22, 1875, 87.
F. da Ponte Horta for $d=7, 9, 11, 13$, Jornal de Sciencias Mat. Ast., 1, 1877, 57-62.
Mennesson for $d=7$, Nouv. Corresp. Math., 4, 1878, 151; generalization by Cesàro, p. 156.
C. Lange, for $d=7, 13, 17, 19$, Ueber die Teilbarkeit der Zahlen, Progr., Berlin, 1879.
F. Jorcke for $d=7, 9, 11$, Ueber Zahlenkongruenzen..., Progr. Fraustadt, 1878.
K. Broda for any base, Archiv Math. Phys., 63, 1879, 413-428.
A. Badoureau for $d=19$, Nouv. Ann. Math., (2), 18, 1879, 35-6.
S. M. Drach for $d=7$, Math. Quest. Educ. Times, 35, 1881, 71-2.
W. A. Pick for $d=7$, *ibid.*, 38, 1883, 64.
A. Evans for $d=7$, Des Moines Analyst, 10, 1883, 134.
K. Haas, Theilbarkeitsregeln..., Progr., Wien, 1883.
G. Wertheim, Elemente der Zahlentheorie, 1887, 31-33.
B. Adam for $d < 100$, Ueber die Teilbarkeit..., Progr. Gym. Clausthal, 1889.
A. Loir for $d < 138$, Jour. de math. élém., 1889, 66, 107-10, 121-3.
A. G. Fazio [Schlegel²⁶], Sui caratteri..., Palermo, 1889.
E. Gelin, Mathesis, (2), 2, 1892, 65, 93; (2), 12, 1902, 65-74, 93-99 (extract in Mathesis, (3), 10, 1910, Suppl. I); Ann. Soc. Sc. Bruxelles, 34, 1909-10, 66; Recueil de problèmes d'arith., 1896. Extracts by M. Nassò, Revue de Math. (ed., Peano), 7, 1900-1, 42-52.
Speckmann, Dorsten, Haas, Dörr, Zeitschrift Math. Phys., 37, 1892, 58, 63, 128, 192, 383.
Lalbaletrier, Jour. de Math. (ed., de Longchamps), 1894, 54.
H. T. Burgess [Pascal⁴], Nature, 57, 1897-8, 8-9, 30, 55.
A. Conti [Pascal⁴], Periodico di Mat., 13, 1898, 180-6, 207-9.
F. Mariantoni, *ibid.*, 149-151, 191-2, 217-8.
T. Lange for $d < 30$, Archiv Math. Phys., (2), 16, 1898, 220-3.
W. J. Greenstreet, Math. Gazette, 1, 1900, 186-7.
Christie for $d=2^np, 5^np$ (p prime), Math. Quest. Educ. Times, 73, 1900, 119.
A. Cunningham and D. Biddle for $d=rp \neq 1$, *ibid.*, 75, 1901, 49-50.
M. Zuccagni for $d=7$, Suppl. al Periodico di Mat., 6, fasc. V.
Calvitti for $d=7$, *ibid.*, 8, fasc. IV.
S. Dickstein, Wiad. Mat., Warsaw, 6, 1902, 253-7 (Polish).
B. Niewenglowski, *ibid.*, 252-3.
Pietzker for $d=7, 11, 13, 27, 37$, Unterrichtsblätter Math. Naturwiss., 9, 1903, 85-110.
A. Church for $d=7, 13, 17$, Amer. Math. Monthly, 12, 1905, 102-3.
E. A. Cazes, Assoc. franç., 36, 1907, 55-63.
A. Gérardin for $d=7, 13, 17, 37, 43$, Sphinx-Oedipe, 1907-8, 2.
M. Morale for $d=7$, Suppl. al Periodico di Mat., 11, 1908, 103.
*T. Ghezzi, *ibid.*, 12, 1908-9, 129-130.
Lenzi, Il Boll. Matematica Gior. Sc.-Didat., 7, 1908.

- R. Polpi, *ibid.*, 8, 1909, 281-5.
 M. Morale for $d=7$, 13, Suppl. al Periodico di Mat., 13, 1909-10, 38-9.
 A. L. Csada, *ibid.*, 56-8.
 *A. La Paglia, *ibid.*, 14, 1910-11, 136-7, extension of Morale to any d .
 A. V. Filippov, 8 methods for $d=9$, Kagans Bote, 1910, 88-92, No. 520.
 P. Cattaneo for $d=11$, Il Boll. Matematica Gior. Sc.-Didat., 9, 1910, 305-6.
 *L. Miceli, Condizioni di divisibilità di un numero N per un numero a . . ., Matera, 1911, 8 pp.
 R. Ayza for $d=a \cdot 10^n \pm 1$, Revista sociedad mat. española, Madrid, 1, 1911, 162-6.
 *Paoletti, Il Pitagora, Palermo, 18, 1911-12, 128-132.
 *R. La Marca, Criteri di congruenza e criteri di divisibilità, Torre del Greco, 1912, 30 pp.
 K. W. Lichteneker, Zeitschr. für Realschulwesen, 37, 1912, 338-49.
 R. E. Cicero, Sociedad Científica Antonio Alzate, 32, 1912-3, 317-331.
 J. G. Galé for $d=7$, Revista sociedad mat. española, 3, 1913-4, 46-7.
 C. F. Iodi for $d=7$, 13, 17, 19, Suppl. al Periodico di Mat., 18, 1914, 20-3.
 E. Kylla for $d=11$, Unterrichtsblätter Math. Naturwiss., 20, 1914, 156.
 R. Krahle for $d=7$, Zeitschrift Math. Naturw. Unterricht, 45, 1914, 562.
 P. A. Fontebasso, Il Boll. Matematica, 13, 1914-5.
 G. M. Persico, Periodico di Mat., 32, 1917, 105-124.
 Sammlung der Aufgaben in Zeitschrift Math. Naturw. Unterricht, 1898: for $d=7$, II, 337; IV, 404, 407; for $d=9$, 11, XXIV, 606; XXV, 587-8; for $d=37$, etc., XXVI, 18, 25-27.
 Criteria for divisibility in connection with tables were given by Barlow,⁴⁸ Tarry⁸⁶ and Lebon⁸⁷ of Ch. XIII, and Harmuth³¹ of Ch. XIV.

PAPERS ON DIVISIBILITY NOT AVAILABLE FOR REPORT.

- Joubin, Jour. Acad. Soc. Sc. France et de l'Etranger, Paris, 2, 1834, 230.
 J. Lenthéric, Théorie de la divisibilité des nombres, Paris, 1838.
 R. Volterrani, Saggio sulla divisione ragionata dei n. interi, Pisa, 1871.
 F. Tirelli, Teoria della divisibilità de' numeri, Napoli, 1875.
 E. Tiberi, Teoria generale sulle condizioni di divisibilità . . ., Arezzo, 1890.
 J. Kroupa, Casopis, Prag, 43, 1914, 117-120.
 G. Schröder, Unterrichtsblätter für Math. Naturwiss., 21, 1915, 152-5.

CHAPTER XIII.

FACTOR TABLES, LISTS OF PRIMES.

Eratosthenes (third century B.C.) gave a method, called the sieve or crib of Eratosthenes, of determining all the primes under a given limit l , which serves also to construct the prime factors of numbers $< l$. From the series of odd numbers 3, 5, 7, . . . , strike out the square of 3 and every third number after 9, then the square of 5 and every fifth number after 25, etc. Proceed until the first remaining number, directly following that one whose multiples were last cancelled, has its square $> l$. The remaining numbers are primes.

Nicomachus and Boethius¹ began with 5 instead of with 5², 7 instead of with 7², etc., and so obtained the prime factors of the numbers $< l$.

A table containing all the divisors of each odd number ≤ 113 was printed at the end of an edition of Aratus, Oxford, 1672, and ascribed to Eratosthenes by the editor, who incorrectly considered the table to be the sieve of Eratosthenes. Samuel Horsley² believed that the table was copied by some monk in a barbarous age either from a Greek commentary on the Arithmetic of Nicomachus or else from a Latin translation of a Greek manuscript, published by Camerarius, in which occurs such a table to 109.

Leonardo Pisano³ gave a table of the 21 primes from 11 to 97 and a table giving the factors of composite numbers from 12 to 100; to determine whether n is prime or not, one can restrict attention to divisors $\leq \sqrt{n}$.

Ibn Albannâ in his Talkhys⁴ (end of 13th century) noted that in using the crib of Eratosthenes we may restrict ourselves to numbers $\leq \sqrt{l}$.

Cataldi⁵ gave a table of all the factors of all numbers up to 750, with a separate list of primes to 750, and a supplement extending the factor table from 751 to 800.

Frans van Schooten⁶ gave a table of primes to 9979.

J. H. Rahn⁷ (Rhonius) gave a table of the least factors of numbers, not divisible by 2 or 5, up to 24000.

T. Brancker⁸ constructed a table of the least divisors of numbers, not divisible by 2 or 5, up to 100 000. [Reprinted by Hinkley.⁵⁵]

¹Introd. in Arith. Nicomachi; Arith. Boethii, lib. 1, cap. 17 (full titles in the chapter on perfect numbers). Extracts of the parts on the crib, with numerous annotations, were given by Horsley.² Cf. G. Bernhardt, *Eratosthenica*, Berlin, 1822, 173-4.

²Phil. Trans. London, 62, 1772, 327-347.

³Il Liber Abbaci di L. Pisano (1202, revised 1228), Roma, 1852, ch. 5; Scritti, 1, 1857, 38.

⁴Transl. by A. Marre, *Atti Accad. Pont. Nuovi Lincei*, 17, 1863-4, 307.

⁵Trattato de' numeri perfetti, Bologna, 1603. *Libri, Histoire des Sciences Math. en Italie*, ed. 2, vol. 4, 1865, 91, stated erroneously that the table extended to 1000.

⁶Exercit. Math., libri 5, cap. 5, p. 394, Leiden, 1657.

⁷Algebra, Zürich, 1659. Wallis,¹⁰ p. 214, attributed this book to John Pell.

⁸An Introduction to Algebra, translated out of the High-Dutch [of Rahn's⁷ Algebra] into English by Thomas Brancker, augmented by D. P. [=Dr. Pell], London, 1668. It is cited in *Phil. Trans. London*, 3, 1668, 688. The Algebra and the translation were described by G. Wertheim, *Bibliotheca Math.*, (3), 3, 1902, 113-126.

D. Schwenter⁹ gave all the factors of the odd numbers < 1000 .

John Wallis¹⁰ gave a list of errata in Brancker's⁸ table.

John Harris,¹¹ D. D., F. R. S., reprinted Brancker's⁸ table.

De Traytorens¹² emphasized the utility of a factor table. To form a table showing all prime factors of numbers to 1000, begin by multiplying 2, 3, . . . by all other primes < 1000 , then multiply 2×3 by all the primes, then $2 \times 3 \times 5$, etc.

Joh. Mich. Poetius¹³ gave a table (*anatomiae numerorum*) of all the prime factors of numbers, not divisible by 2, 3, 5, up to 10200. It was reprinted by Christian Wolf,¹⁴ Willigs,¹⁹ and Lambert.²²

Johann Gottlob Krüger¹⁵ gave a table of primes to 100 999 (not to 1 million, as in the title), stating that the table was computed by Peter Jäger of Nürnberg.

James Dodson¹⁶ gave the least divisors of numbers to 10000 not divisible by 2 or 5 and the primes from 10000 to 15000.

Etienne François du Tour¹⁷ described the construction of a table of all composite odd numbers to 10000 by multiplying 3, 5, . . . , 3333 by 3, . . . , 99.

Giuseppe Pigri¹⁸ gave all prime factors of numbers to 10000.

Michel Lorenz Willigs¹⁹ (Willich) gave all divisors of numbers to 10000.

Henri Anjema²⁰ gave all divisors of numbers to 10000.

Rallier des Ourmes²¹ gave as if new the sieve of Eratosthenes, placing 3 above 9 and every third odd number after it, a 7 above 49, etc. He expressed each number up to 500 as a product of powers of primes.

J. H. Lambert²² described a method of making a factor table and gave Poetius's¹³ table and expressed a desire for a table to 102 000. Lagrange called his attention to Brancker's⁸ table.

Lambert²³ gave [Krüger's¹⁵] table showing the least factor of numbers not divisible by 2, 3, 5 up to 102000, and a table of primes to 102 000, errata in which were noted by Klügel²⁴.

⁹*Geometria Practica*, Nurnb., 1667, I, 312.

¹⁰*Treatise of Algebra*, additional treatise, Ch. III, §22, London, 1685.

¹¹*Lexicon Technicum*, or an Universal English Dictionary of Arts and Sciences, London, vol. 2, 1710 (under *Incomposite Numbers*). In ed. 5, London, 2, 1736, the table was omitted, but the text describing it kept. Wallis, *Opera*, 2, 511, listed 30 errors.

¹²*Histoire de l'Acad. Roy. Science*, année 1717, Paris, 1741, Hist., 42–47.

¹³*Anleitung zu der Arith. Wissenschaft vermittelst einer parallel Algebra*, Frkf. u. Leipzig, 1728.

¹⁴*Vollst. Math. Lexicon*, 2, Leipzig, 1742, 530.

¹⁵*Gedanken von der Algebra*, nebst den Primzahlen von 1 bis 1 000 000, Halle im Magd., 1746. Cf. Lambert.²²

¹⁶*The Calculator . . . Tables for Computation*, London, 1747.

¹⁷*Histoire de l'Acad. Roy. Sc.*, Paris, année 1754, Hist., 88–90.

¹⁸*Nuove tavole degli elementi dei numeri dall' 1 al 10 000*, Pisa, 1758.

¹⁹*Gründliche Vorstellung der Reesischen allgemeinen Regel . . . Rechnungsarten*, Bremen u. Göttingen, 2, 1760, 831–976.

²⁰*Table des diviseurs de tous les nombres naturels*, depuis 1 jusqu'à 10 000, Leyden, 1767, 302 pp.

²¹*Mém. de math. et de physique*, Paris, 5, 1768, 485–499.

²²*Beyträge zum Gebrauche der Math. u. deren Anwendung*, Berlin, 1770, II, 42.

²³*Zusätze zu den logarithmischen und trig. Tabellen*, Berlin, 1770.

²⁴*Math. Wörterbuch*, 3, 1808, 892–900.

J. Ozanam²⁵ gave a table of primes to 10000.

A. F. Marci²⁶ gave in 1772 a list of primes to 400 000.

Jean Bernoulli^{26a} tabulated the primes $16n+1$ up to 21601.

L. Euler²⁷ discussed the construction of a factor table to one million. Given a prime $p=30a\pm t$ ($t=1, 7, 11, 13$), he determined for each $r=1, 7, 11, 13, 17, 19, 23, 29$, the least q for which $30q+r$ is divisible by p , and arranged the results in a single table with p ranging over the primes from 7 to 1000. He showed how to use this auxiliary table to construct a factor table between given limits.

C. F. Hindenburg²⁸ employed in the construction of factor tables a "patrone" or strip of thick paper with holes at proper intervals to show the multiples of p , for the successive primes p .

A. Felkel²⁹ gave in 1776 a table of all the prime factors (designated by letters or pairs of letters) of numbers, not divisible by 2, 3, or 5, up to 408 000, requiring for entry two auxiliary tables. In manuscript³⁰, the table extended to 2 million; but as there were no purchasers of the part printed, the entire edition, except for a few copies, was used for cartridges in the Turkish war. The imperial treasury at Vienna, at the cost of which the table was printed, retained the further manuscript. [See Felkel.³⁸]

L. Bertrand³¹ discussed the construction of factor tables.

The *Encyclopédie* of d'Alembert, ed. 1780, end of vol. 2, contains a factor table to 100 000.

Franz Schaffgotsch³² gave a method, equivalent to that of a stencil for each prime p , for entering the factor p in a factor table with eight headings $30m+k$, $k=1, 7, 11, 13, 17, 19, 23, 29$, and hence of numbers not divisible by 2, 3, or 5. Proofs were given by Beguelin and Tessanek, *ibid.*, 362, 379.

The strong appeals by Lambert²³ that some one should construct a factor table to one million led L. Oberreit, von Stamford, Rosenthal, Felkel, and Hindenburg to consider methods of constructing factor tables and to prepare such tables to one million, with plans for extension to 5 or 10

²⁵Recreations Math., new ed., Paris, 1723, 1724, 1735, etc., I, p. 47.

²⁶Primes "in quater centenis millibus," Amstelodami, 1772.

^{26a}Nouv. Mém. Ac. Berlin, année 1771, 1773, 323.

²⁷Novi Comm. Acad. Petrop., 19, 1774, 132; Comm. Arith., 2, 64.

²⁸Beschreibung einer ganz neuen Art nach einem bekannten Gesetze fortgehende Zahlen durch Abzählen oder Abmessen bequem u. sicher zu finden. Nebst Anwendung der Methode auf verschiedene Zahlen, besonders auf eine darnach zu fertigende Factorentafel..., Leipzig, 1776, 120 pp.

²⁹Tabula omnium factorum simplicium, numerorum per 2, 3, 5 non divisibilium ab 1 usque 10 000 000 [!]. Elaborata ab Antonio Felkel. Pars I. Exhibens factores ab 1 usque 144 000, Vindobonae, 1776. Then there is a table to 408 000, given in three sections. There is a copy of this complete table in the Graves Library, University College, London. Tafel aller einfachen Factoren der durch 2, 3, 5 nicht theilbaren Zahlen von 1 bis 10 000 000. Entworfen von Anton Felkel. I. Theil. Enthaltend die Factoren von 1 bis 144 000, Wien, 1776. There is a copy of this incomplete table in the libraries of the Royal Society of London and Göttingen University.

³⁰Cf. Zach's Monatliche Correspondenz, 2, 1800, 223; Allgemeine deutsche Bibliothek, 33, II, 495.

³¹Dévelop. nouveau de la partie él. math., Genève, 1774.

³²Gesetz, welches zur Fortsetzung der bekannten Pellischen Tafeln dient, Abhand. Privatgesellschaft in Böhmen, Prag, 5, 1782, 354-382.

million. Their extended correspondence with Lambert³³ was published. Of the tables constructed by these computers, the only one published is that by Felkel.²⁹ The history of their connection with factor tables has been treated by J. W. L. Glaisher.³⁴

Johann Neumann³⁵ gave all the prime factors of numbers to 100 100.

Desfaviaae gave a like table in the same year.

F. Maseres³⁶ reprinted the table of Brancker.⁸

G. Vega³⁷ gave all the prime factors of numbers not divisible by 2, 3, or 5 to 102 000 and a list of primes from 102 000 to 400 031. Chernac listed errors in both tables. In Hülse's edition, 1840, of Vega, the list of primes extends to 400 313.

A. Felkel,³⁸ in his Latin translation of Lambert's²³ *Zusätze*, gave all the prime factors except the greatest of numbers not divisible by 2, 3, 5 up to 102 000, large primes being denoted by letters. In the preface he stated that, being unable to obtain his extensive manuscript³⁰ in 1785, he calculated again a factor table from 408 000 to 2 856 000.

J. P. Gruson³⁹ gave all prime factors of numbers not divisible by 2, 3, 5 to 10500. He^{39a} gave a table of primes to 10000.

F. W. D. Snell⁴⁰ gave the prime factors of numbers to 30000.

A. G. Kästner⁴¹ gave a report on factor tables.

K. C. F. Krause⁴² gave a table of 22 pages showing all products $< 100\,000$ of two primes, a table of primes $< 100\,000$ with letters for 01, 03, . . . , 99, and (pp. 25–28) a factor table to 10000 by use of letters for numbers < 100 .

N. J. Lidonne⁴³ gave all prime factors of numbers to 102 000.

Jacob Struve^{43a} made a factor table to 100 by de Traytorens'¹² method.

L. Chernac⁴⁴ gave all the prime factors of numbers, not divisible by 2, 3 or 5, up to 1 020 000.

J. C. Burckhardt⁴⁵ gave the least factor of numbers to 3 million. He did not compute the first million, but compared Chernac's table with a manuscript (mentioned in Briefwechsel,³³ p. 140) by Schenmarck which extended to 1 008 000. Cf. Meissel.⁶⁶

³³Joh. Heinrich Lamberts deutscher gelehrter Briefwechsel, herausgegeben von Joh. Bernoulli, Berlin, 1785, Leipzig, 1787, vol. 5. ³⁴Proc. Cambridge Phil. Soc., 3, 1878, 99–138.

³⁵Tabellen der Primzahlen und der Faktoren der Zahlen, welche unter 100 100, und durch 2, 3 oder 5 nicht theilbar sind, Dessau, 1785, 200 pp.

³⁶The Doctrine of Permutations and Combinations . . . , London, 1795.

³⁷Tabulæ logarithmico-trigonometricæ, 1797, vol. 2.

³⁸J. H. Lambert, Supplementa tab. log. trig., Lisbon, 1798.

³⁹Pinacothèque, ou collection de Tables . . . , Berlin, 1798.

^{39a}Enthüllte Zaubereyen u. Geheimnisse d. Arith., Berlin, 1796, I, 82–4.

⁴⁰Ueber eine neue und bequeme Art, die Factorentafeln einzurichten, nebst einer Kupfertafel der einfachen Factoren von 1 bis 30000, Giessen und Darmstadt, 1800.

⁴¹Fortsetzung der Rechenkunst, ed. 2, Göttingen, 1801, 566–582.

⁴²Factoren- und Primzahlentafel von 1 bis 100 000 neu berechnet, Jena u. Leipzig, 1804.

⁴³Tables de tous les diviseurs des nombres $< 102\,000$, Paris, 1808.

^{43a}Handbuch der Math., Altona, II, 1809, 108.

⁴⁴Cribrum Arithmeticum . . . Daventriæ, 1811, 1020 pp. Reviewed by Gauss, Göttingische gelehrte Anzeigen, 1812; Werke 2, 181–2. Errata, Cunningham.⁶⁵

⁴⁵Tables des diviseurs . . . 1 à 3 036 000, Paris, 1817, 1814, 1816 (for the respective three millions), and 1817 (in one volume).

P. Barlow⁴⁶ gave the prime and power of prime factors of numbers to 10000 and a list of primes to 100 103.

C. Hutton⁴⁷ gave the least factor of numbers to 10000.

Rees' Cyclopaedia, 1819, vol. 28, lists the primes to 217 219.

Peter Barlow⁴⁸ gave a two-page table for finding factors of a number $N < 100\,000$. The primes $p = 7$ to $p = 313$ are at the head of the columns, while the 18 numbers 1000, . . . , 9000, 10000, 20000, . . . , 90000 are in the left-hand column. In the body of the table is the remainder of each of the latter when divided by the primes p . To test if p is a factor of N , add its last two digits to the remainders in the line of hundreds and thousands in the column headed p and test whether the sum is divisible by p .

J. P. Kulik⁴⁹ gave a factor table to 1 million.

J. Hantschl⁵⁰ gave a factor table to 18277; J. M. Salomon,⁵¹ to 102 011.

A. L. Crelle⁵² gave the number of primes $4n + 1$ and the number of primes $4n + 3$ in each thousand up to the fiftieth.

A. Guyot⁵³ listed the primes to 100 000.

A. F. Möbius,^{53a} using square ruled paper, inserted from right to left 0, 1, 2, . . . in the top row of cells, and inserted n in each cell of the n th row below the top row whenever the corresponding number in the top row is divisible by n . We thus have a factor table. Certain numbers of the table lie in straight lines, others in parabolas, etc.

P. A. G. Colombier^{53b} discussed the determination of the primes $< l'$, given those $< l$.

H. G. Köhler⁵⁴ gave a factor table to 21524.

E. Hinkley⁵⁵ gave a factor table to 100 000, listing all factors of odd numbers to 20000 and of even numbers to 12500.

F. Schallen^{55a} gave the prime and prime-power factors of numbers < 10000 .

F. Landry⁵⁶ gave factor and prime tables to 10000.

A. L. Crelle⁵⁷ discussed the expeditious construction of a factor table, and in particular a method of extending Chernac's⁴⁴ table to 7 million.

J. Hoüel⁵⁸ gave a factor table to 10841.

Jacob Philip Kulik (1773–1863) spent 20 years constructing a factor

⁴⁶New Mathematical Tables, London, 1814. Errata, Cunningham.⁸⁵

⁴⁷Phil. and Math. Dictionary, 1815, vol. 2, 236–8.

⁴⁸New Series of Math. Repository (ed., Th. Leybourn), London, 4, 1819, II, 30–39.

⁴⁹Tafeln der einfachen Faktoren aller Zahlen unter 1 million, Graz, 1825.

⁵⁰Log.-trig. Handbuch, Wien, 1827.

⁵¹Log. Tafeln, Wien, 1827.

⁵²Jour. für Math., 10, 1833, 208.

⁵³Théorie générale de la divisibilité des nombres, suivie d'applications variées et d'une table de nombres premiers compris entre 0 et 100 000, Paris, 1835.

^{53a}Jour. für Math., 22, 1841, 276–284.

^{53b}Nouv. Ann. Math., 2, 1843, 408–410.

⁵⁴Log.-trig. Handbuch, Leipzig, 1848. Errata, Cunningham.⁸⁵

⁵⁵Tables of the prime numbers and prime factors of the composite numbers from 1 to 100 000, Baltimore, 1853. Reproduction of Brancker's⁸ table.

^{55a}Primzahlen-Tafel von 1 bis 10000 . . . , Weimar, 1855. For 99 errata, see Cunningham.⁸⁵

⁵⁶Tables des nombres entiers non divisibles par 2, 3, 5, et 7, jusqu'à 10201, avec leurs diviseurs simples en regard, et des carrés des 1000 premiers nombres, Paris, 1855. Tables des nombres premiers, de 1 à 10000, Paris, 1855.

⁵⁷Jour. für Math., 51, 1856, 61–99.

⁵⁸Tables de log., Paris, 1858.

table to 100 million; the manuscript⁵⁹ has been in the library of the Vienna Royal Academy since 1867. Lehmer⁹² gave an account of the first of the eight volumes of the manuscript, listed 226 errors in the tenth million, and concluded that Kulik's manuscript is certainly not accurate enough to warrant publication, though of inestimable value in checking a newly constructed table. Lehmer⁹⁵ gave a further account of this manuscript which he examined in Vienna. Volume 2, running from 12 642 600 to 22 852 800 is missing. The eight volumes contained 4,212 pages.

B. Goldberg⁶⁰ gave all factors of numbers prime to 2, 3, 5, to 251 647.

Zacharias Dase,⁶¹ in the introduction to the table for the seventh million, printed a letter from Gauss, dated 1850, giving a brief history of previous tables and referring to the manuscript factor table for the fourth, fifth and sixth millions presented to the Berlin Academy by A. L. Crelle. Although Gauss was confident this manuscript would be published, and hence urged Dase to undertake the seventh million, etc., the Academy found the manuscript to be so inaccurate that its publication was not advisable. Dase died in 1861 leaving the seventh million complete and remarkably accurate, the eighth nearly complete, and a large part of the factors for the ninth and tenth millions. The work was completed by Rosenberg, but with numerous errors. The table for the tenth million has not been printed; the manuscript was presented to the Berlin Academy in 1878, but no trace of it was found when Lehmer⁹² desired to compare it with his table of 1909.

C. F. Gauss⁶² gave a table showing the number of primes in each thousand up to one million and in each ten thousand from one to three million, with a comparison with the approximate formula $\int dx/\log x$.

V. A. Lebesgue⁶³ discussed the formation of factor tables and gave that to 115 500 constructed by Hoüel.

W. H. Oakes⁶⁴ used a complicated apparatus consisting of three tables on six sheets of various sizes and nine perforated cards (cf. Committee,⁶⁸ p. 39).

W. B. Davis⁶⁵ considered numbers in the vicinity of 10^8 , and of 10^{11} .

E. Meissel⁶⁶ computed the number of primes in the successive sets of 100 000 numbers to one million and concluded that Burekhardt's⁴⁵ table gives correctly the primes to one million.

⁵⁹Cited by Kulik, *Abh. Böhm. Gesell. Wiss., Prag*, (5), 11, 1860, 24, footnote. A report on the manuscript was made by J. Petzval, *Sitzungsberichte Ak. Wiss. Wien (Math.)*, 53, 1866, II, 460. Cited by J. Perott, *l'intermédiaire des math.*, 2, 1895, 40; 11, 1904, 103.

⁶⁰*Primzahlen- u. Faktortafeln von 1 bis 251 647*, Leipzig, 1862. Errata, Cunningham.⁸⁵

⁶¹*Factoren-Tafeln für alle Zahlen der siebenten Million . . .*, Hamburg, 1862; . . . *der achten Million*, 1863; . . . *der neunten Million (ergänzt von H. Rosenberg)*, 1865.

⁶²Posthumous manuscript, *Werke*, 2, 1863, 435-447.

⁶³*Tables diverses pour la décomposition des nombres en leurs facteurs premiers*, *Mém. soc. sc. phys. et nat. de Bordeaux*, 3, cah. 1, 1864, 1-37.

⁶⁴Machine table for determining primes and the least factors of composite numbers up to 100 000, London, 1865.

⁶⁵*Jour. de Math.*, (2), 11, 1866, 188-190; *Proc. London Math. Soc.*, 4, 1873, 416-7. *Math. Quest. Educ. Times*, 7, 1867, 77; 8, 1868, 30-1.

⁶⁶*Math. Annalen*, 2, 1870, 636-642. Cf. 3, p. 523; 21, 1883, p. 304; 25, 1885, p. 251.

J. W. L. Glaisher⁶⁷ gave for the second and ninth millions the number of primes in each interval of 50000 and a comparison with $li x' - li x$, where $li x = \int dx / \log x$ [more precise definition at the end of Ch. XVIII].

A committee⁶⁸ consisting of Cayley, Stokes, Thompson, Smith, and Glaisher prepared the Report on Mathematical Tables, which includes (pp. 34-9) a list of factor and prime tables.

J. W. L. Glaisher⁶⁹ described in detail the method used by his father⁷⁰ and gave an account of the history of factor tables.

Glaisher^{69a} enumerated the primes in the tables of Burckhardt and Dase.

Glaisher^{69b} tabulated long sets of consecutive composite numbers. He^{69c} enumerated the prime pairs (as 11, 13) in each successive thousand to 3 million and in the seventh, eighth, and ninth millions.

E. Lucas^{69d} wrote $P(q)$ for the product of all the primes $\leq q$, where q is the largest prime $< n$. If $xP(q) \pm 1$ are both composite, $xP(q) - n, \dots, xP(q), \dots, xP(q) + n$ give $2n + 1$ composite numbers.

Glaisher^{69e} enumerated the primes $4n + 1$ and the primes $4n + 3$ for intervals of 10000 in the k th million for $k = 1, 2, 3, 7, 8, 9$.

James Glaisher⁷⁰ filled the gap between the tables by Burckhardt⁴⁵ and Dase⁶¹. The introduction to the table for the fourth million gives a history of factor tables and their construction. Lehmer⁹² praised the accuracy of Glaisher's table, finding in the sixth million a single error besides two misprints.

Tuxen⁷¹ gave a process to construct tables of primes.

Groscurth and Gudila-Godlewski, Moscow, 1881, gave factor tables.

*V. Bouniakowsky^{71a} gave an extension of the sieve of Eratosthenes.

W. W. Johnson^{71b} repeated Glaisher's⁷⁰ remarks on the history of tables.

P. Seelhoff⁷² gave large primes $k \cdot 2^n + 1$ ($k < 100$) and composite cases.

Simony⁷³ gave the digits to base 2 of primes to $2^{14} = 16384$.

L. Saint-Loup⁷⁴ gave a graphical exposition of Eratosthenes' sieve.

H. Vollprecht⁷⁵ discussed the construction of factor tables.

⁶⁷Report British Association for 1872, 1873, trans., 19-21. Cf. W. W. Johnson, Des Moines Analyst, 2, 1875, 9-11.

⁶⁸Report British Association for 1873, 1874, pp. 1-175. Continued in 1875, 305-336; French transl., Sphinx-Oedipe, 8, 1913, 50-60, 72-79; 9, 1914, 8-14.

⁶⁹Proc. Cambridge Phil. Soc., 3, 1878, 99-138, 228-9.

^{69a}*Ibid.*, 17-23, 47-56; Report British Assoc., 1877, 20 (sect.). Extracts by W. W. Johnson, Des Moines Analyst, 5, 1878, 7.

^{69b}Messenger Math., 7, 1877-8, 102-6, 171-6; French transl., Sphinx-Oedipe, 7, 1912, 161-8.

^{69c}*Ibid.*, 8, 1879, 28-33.

^{69d}*Ibid.*, p. 81. C. Gill, Ladies' Diary, 1825, 36-7, had noted that $xP(q) + j$ is composite for $j = 2, \dots, q - 1$.

^{69e}Report British Assoc., 1878, 470-1; Proc. Roy. Soc. London, 29, 1879, 192-7.

⁷⁰Factor tables for the fourth, fifth and sixth millions, London, 1879, 1880, 1883.

⁷¹Tidsskrift for Mat., (4), 5, 1881, 16-25.

^{71a}Memoirs Imperial Acad. Science, St. Petersburg, 41, 1882, Suppl., No. 3, 32 pp.

^{71b}Annals of Math., 1, 1884-5, 15-23.

⁷²Zeitschrift Math. Phys., 31, 1886, 380. Reprinted, Sphinx-Oedipe, 4, 1909, 95-6.

⁷³Sitzungsber. Ak. Wiss. Wien (Math.), 96, II, 1887, 191-286.

⁷⁴Comptes Rendus Paris, 107, 1888, 24; Ann. de l'école norm., (3), 7, 1890, 89-100.

⁷⁵Ueber die Herstellung von Faktorentafeln, Diss. Leipzig, 1891.

C. A. Laisant^{75a} would exhibit a factor table by use of shaded and unshaded squares on square-ruled paper without using numbers for entries.

G. Speckmann^{75b} made trivial remarks on the construction of a list of primes.

P. Valerio⁷⁶ arranged the odd numbers prime to 5 in four columns according to the endings 1, 3, 7, 9. From the first column cross out the first multiple 21 of 3, then the third following number 51, etc. Similarly for the other columns. Then use the primes 7, 11, etc., instead of 3.

J. P. Gram⁷⁷ published the computation by N. P. Bertelsen of the number of primes to ten million in intervals of 50000 or less, which led to the detection of numerous errors in the tables of Burckhardt⁴⁵ and Dase.⁶¹

G. L. Bourgerel⁷⁸ gave a table with 0, 1, . . . , 9 in the first row, 10, . . . , 19 in the second row (with 10 under 0), etc. Then all multiples of a chosen number lie in straight lines forming a parallelogram lattice, with one branch through 0. For example, the multiples of 3 appear in the line through 0, 12, 24, 36, . . . , the parallel through 3, 15, 27, . . . , the parallel 21, 33, 45, . . . ; also in a second set of parallels 3, 12, 21, 30; 6, 15, 24, 33, 42, 51, 60; etc.

E. Suchanek⁷⁹ continued to 100 000 Simony's⁷³ table of primes to base 2.

D. von Sterneck⁸⁰ counted the number of primes $100n+1$ in each tenth of a million up to 9 million and noted the relatively small variation from one-fortieth of the total number of primes in the interval.

H. Vollprecht⁸¹ discussed the determination of the number of primes $< N$ by use of the primes $< \sqrt{N}$.

A. Cunningham and H. J. Woodall⁸² discussed the problem to find all the primes in a given range and gave many successive primes > 9 million. They^{82a} listed 117 primes between $2^{24} \pm 1020$.

H. Schapira^{82b} discussed algebraic operations equivalent to the sieve of Eratosthenes.

*V. Di Girio, Alba, 1901, applied indeterminate analysis of the first degree to define a new sieve of Eratosthenes and to factoring.

John Tennant⁸³ wrote numbers to the base 900 and used auxiliary tables.

A. Cunningham^{83a} gave long lists of primes between $9 \cdot 10^6$ and 10^{11} .

Ph. Jolivald⁸⁴ noted that a table of all factors of the first $2n$ numbers serves to tell readily whether a number $< 4n+2$ is prime or not.

^{75a}Assoc. franç., 1891, II, 165-8.

^{75b}Archiv Math. Phys., (2), 11, 1892, 439-441.

⁷⁶La revue scientifique de France, (3), 52, 1893, 764-5.

⁷⁷Acta Math., 17, 1893, 301-314. List of errors reproduced in Sphinx-Oedipe, 5, 1910, 49-51.

⁷⁸La revue scientifique de France, (4), 1, 1894, 411-2.

⁷⁹Sitzungsber. Ak. Wiss. Wien (Math.), 103, II a, 1894, 443-610.

⁸⁰Anzeiger K. Akad. Wiss. Wien (Math.), 31, 1894, 2-4. Cf. Kronecker, p. 416 below.

⁸¹Zeitschrift Math. Phys., 40, 1895, 118-123.

⁸²Report British Assoc., 1901, 553; 1903, 561; Messenger Math., 31, 1901-2, 165; 34, 1904-5, 72, 184; 37, 1907-8, 65-83; 41, 1911, 1-16.

^{82a}Report British Assoc., 1900, 646.

^{82b}Jahresber. d. Deutschen Math. Verein., 5, 1901, I, 69-72.

⁸³Quar. Jour. Math., 32, 1901, 322-342.

^{83a}*Ibid.*, 35, 1903, 10-21; Mess. Math., 36, 1907, 145-174; 38, 1908, 81-104; 38, 1909, 145-175; 39, 1909, 33-63, 97-128; 40, 1910, 1-36; 45, 1915, 49-75; Proc. London Math. Soc., 27, 1896, 327; 28, 1897, 377-9; 29, 1898, 381-438, 518; 34, 1902, 49.

⁸⁴L'intermédiaire des math., 11, 1904, 97-98.

A. Cunningham⁸⁵ noted errata in various factor tables.

*J. R. Akerlund^{85a} discussed the determination of primes by a machine.

Gaston Tarry⁸⁶ would use an auxiliary table (as did Barlow in 1819) to tell by the addition of two entries ($< \frac{1}{2}p$) if a given number $< N$ is divisible by a chosen prime p . For $N=10000$, he used the base $b=100$, and gave a table showing the numerically least residues of the numbers $r < b$ and the multiples of b for each prime $p < b$. Then $nb+r$ is divisible by p if the residues of nb and r are equal and of opposite sign. For $N=100\,000$, he used $b=60060=2\cdot 91\cdot 330$ and wrote numbers in the form $mb+330q+r$, $q < 90$, $r < 330$; or, again, $b=20580$. Ernest Lebon⁸⁷ used such tables with the base $30030=2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13$, or its product by 17.

Ernest Lebon,⁸⁸ J. Deschamps,⁸⁹ and C. A. Laisant^{89a} discussed the construction of factor tables.

J. C. Morehead⁹⁰ extended the sieve of Eratosthenes to numbers ma^k+b ($m=1, 2, 3, \dots$) in any arithmetical progression. The case $a=2$, $b=\pm 1$, is discussed in detail, with remarks on the construction of a table to serve as a factor table for numbers $m\cdot 2^k \pm 1$.

L. L. Dines⁹¹ treated the case $a=6$, $b=\pm 1$, and the factorization of numbers $m\cdot 6^k \pm 1$.

D. N. Lehmer⁹² gave a factor table to 10 million and listed the errata in the tables by Burckhardt, Glaisher, Dase, Dase and Rosenberg, and Kulik's tenth million, and gave references to other (shorter) lists of errata.

E. B. Escott^{92a} listed 94 pairs of consecutive large numbers all of whose prime factors are small.

L. Aubry^{92b} proved that a group of 30 consecutive odd numbers does not contain more than 15 primes or numbers all of whose prime factors exceed 7.

Cunningham^{92c} listed the numbers of 5 digits with prime factors ≤ 11 .

⁸⁵Messenger Math., 34, 1904-5, 24-31; 35, 1905-6, 24.

^{85a}Nyt Tidsskrift for Mat., Kjobenhavn, 16A, 1905, 97-103.

⁸⁶Bull. Soc. Philomathique de Paris, (9), 8, 1906, 174-6, 194-6; 9, 1907, 56-9. Sphinx-Oedipe, Nancy, 1906-7, 39-41. Tablettes des Cotes, Gauthier-Villars, Paris, 1906. Assoc. franç. avanc. sc., 36, 1907, II, 32-42; 41, 1912, 38-43.

⁸⁷Comptes Rendus Paris, 151, 1905, 78. Bull. Amer. Math. Soc., 13, 1906-7, 74. L'enseignement math., 9, 1907, 185. Bull. Soc. Philomathique de Paris, (9), 8, 1906, 168, 270; (9), 10, 1908, 4-9, 66-83; (10), 2, 1910, 171-7. Assoc. franç. avanc. sc., 36, 1907, II, 11-20, 49-55; 37, 1909, 33-6; 41, 1912, 44-53; 43, 1914, 29-35. Rend. Accad. Lincei, Rome, (5), 15, 1906, I, 439; 26, 1917, I, 401-5. Sphinx-Oedipe, 1908-9, 81, 97. Bull. Sc. Math. Élé., 12, 1907, 292-3. Il Pitagora, Palermo, 13, 1906-7, 81-91 (table serving to factor numbers from 30030 to 510 510). Table de caractéristiques relatives à la base 2310 des facteurs premiers d'un nombre inférieur à 30030, Paris, 1906, 32 pp. Comptes Rendus Paris, 159, 1914, 597-9; 160, 1915, 758-760; 162, 1916, 346-8; 163, 1916, 259-261; 164, 1917, 482-4.

⁸⁸Jornal de sciencias math., phys. e nat., acad. sc. Lisboa, (2), 7, 1906, 209-218.

⁸⁹Bull. Soc. Philomathique de Paris, (9), 9, 1907, 112-128; 10, 1908, 10-41.

^{89a}Assoc. franç., 41, 1912, 32-7.

⁹⁰Annals of Math., (2), 10, 1908-9, 88-104.

⁹¹Ibid., pp. 105-115.

⁹²Factor table for the first ten millions, Carnegie Inst. Wash. Pub. No. 105, 1909.

^{92a}Quar. Jour. Math., 41, 1910, 160-7; l'intermédiaire des math., 11, 1904, 65; Math. Quest. Educ. Times, (2), 7, 1905, 81-5.

^{92b}Sphinx-Oedipe, 6, 1911, 187-8; Problem of Lionnet, Nouv. Ann. Math., (3), 2, 1883, 310.

^{92c}Math. Quest. Educ. Times, (2), 21, 1912, 82-3.

E. Lebon⁹³ stated that he constructed in 1911 a table of residues ρ, ρ' permitting the rapid factorization of numbers to 100 million, the manuscript being in the Bibliothèque de l'Institut.

H. W. Stager⁹⁴ gave theorems on numbers which contain no factors of the form $p(kp+1)$, where $k > 0$ and p is a prime, and listed all such numbers < 12230 .

Lehmer⁹⁵ listed the primes to ten million.

A. Gérardin⁹⁶ discussed the finding of all primes between assigned limits by use of stencils for 3, 5, 7, 11, He⁹⁷ described his manuscript of an auxiliary table permitting the factoring of numbers to 200 million. He^{98a} gave a five-page table serving to factor numbers of the second million. Corresponding to each prime $M \leq 14867$ is an entry P such that $N = 1\,000\,000 + P$ is divisible by M . If a value of P is not in the table, N is prime (the P 's range up to 28719 and are not in their natural order). By a simple division one obtains the least odd number in any million which is divisible by the given prime $M \leq 14867$.

C. Boulogne⁹⁸ made use of lists of residues modulus 30 and 300.

H. E. Hansen⁹⁹ gave an impracticable method of forming a table of primes based on the fact that all composite numbers prime to 6 are products of two numbers $6x \pm 1$, while such a product is $6N \pm 1$, where $N = 6xy \pm x + y$ or $6xy - x - y$. A table of values of these N 's up to k serves to find the composite numbers up to $6k$. To apply this method to factor $6N \pm 1$, seek an expression for N in one of the above three forms.

N. Alliston¹⁰⁰ described a sieve (a modification of that by Eratosthenes) to determine the primes $4n+1$ and the primes $4n-1$.

H. W. Stager¹⁰¹ expressed each number < 12000 as a product of powers of primes, and for each odd prime factor gave the values > 0 of k for all divisors of the form $p(kp+1)$. The table thus gives a list of numbers which include the numbers of Sylow subgroups of a group of order ≤ 12000 .

In Ch. XVI are cited the tables of factors of a^2+1 by Euler,^{4, 7} Escott,⁵⁸ Cunningham⁶³ and Woodall⁶⁴; those of a^2+k^2 ($k=1, \dots, 9$) of Gauss¹³; those of y^n+1 , $y^4 \pm 2$, $y^y \pm 1$, $x^y \pm y^x$, $2^q \pm q$, etc., of Cunningham.^{68, 84-9} Concerning the sieve of Eratosthenes, see Noviomagus²⁹ of Ch. I, Poretzky⁶⁶ of Ch. V, Merlin¹³⁹ and de Polignac³⁰⁵⁻⁷ of Ch. XVIII. Saint-Loup¹³ of Ch. XI, Raymond¹⁵¹ and Kempner¹⁵² of Ch. XIV, represented graphically the divisors of numbers, while Kulik¹³⁴ gave a graphical determination of primes.

⁹³L'intermédiaire des math., 19, 1912, 237.

⁹⁴University of California Public. in Math., 1, 1912, No. 1, 1-26.

⁹⁵List of prime numbers from 1 to 10,006,721. Carnegie Inst. Wash. Pub. No. 165, 1914. The introduction gives data on the distribution of primes.

⁹⁶Math. Gazette, 7, 1913-4, 192-3.

⁹⁷Assoc. franç. avanc. sc., 42, 1913, 2-8; 43, 1914, 26-8.

⁹⁸Ibid., 43, 1914, 17-26.

^{98a}Sphinx-Oedipe, série spéciale, No. 1, Dec., 1913.

⁹⁹L'enseignement math., 17, 1915, 93-9. Cf. pp. 244-5 for remarks by Gérardin.

¹⁰⁰Math. Quest. Educat. Times, 28, 1915, 53.

¹⁰¹A Sylow factor table of the first twelve thousand numbers. Carnegie Inst. Wash. Pub. No. 151, 1916.

CHAPTER XIV.

METHODS OF FACTORING.

FACTORING BY METHOD OF DIFFERENCE OF TWO SQUARES.

Fermat¹ described his method as follows: "An odd number not a square can be expressed as the difference of two squares in as many ways as it is the product of two factors, and if the squares are relatively prime the factors are. But if the squares have a common divisor d , the given number is divisible by d and the factors by \sqrt{d} . Given a number n , for example 2027651281, to find if it be prime or composite and the factors in the latter case. Extract the square root of n . I get $r=45029$, with the remainder 40440. Subtracting the latter from $2r+1$, I get 49619, which is not a square in view of the ending 19. Hence I add $90061=2+2r+1$ to it. Since the sum 139680 is not a square, as seen by the final digits, I again add to it the same number increased by 2, *i. e.*, 90063, and I continue until the sum becomes a square. This does not happen until we reach 1040400, the square of 1020. For by an inspection of the sums mentioned it is easy to see that the final one is the only square (by their endings except for 499944). To find the factors of n , I subtract the first number added, 90061, from the last, 90081. To half the difference add 2. There results 12. The sum of 12 and the root r is 45041. Adding and subtracting the root 1020 of the final sum 1040400, we get 46061 and 44021, which are the two numbers nearest to r whose product is n . They are the only factors since they are primes. Instead of 11 additions, the ordinary method of factoring would require the division by all the numbers from 7 to 44021."

Under Fermat,³¹⁷ Ch. I, was cited Fermat's factorization of the number 100895598169 proposed to him by Mersenne in 1643.

C. F. Kausler² would add $1^2, 2^2, \dots$ to N to make the sum a square.

C. F. Kausler³ proceeded as follows to express $4m+1$ in the form p^2-q^2 . Then q is even, $q=2Q$. Set $p-q=2\beta+1$. Then $m=Q(2\beta+1)+\beta(\beta+1)$. Subtract from m in turn the pronic numbers $\beta(\beta+1)$, a table of which he gave on pp. 232-267, until we reach a difference divisible by $2\beta+1$.

Ed. Collins,⁴ in factoring N by expressing it as a difference of two squares, let g^2 be the least odd or even square $>N$, according as $N \equiv 1$ or $3 \pmod{4}$, and set $N=g^2-r$. If r is not a square, set $r=h^2-c$, where h^2 is the even or odd square just $>r$, according as r is even or odd, whence $c=4d$, $N=g^2-h^2+4d$. By trial find integers x, y such that both g^2+x and h^2+y are squares, while $x-y=4d$. Then N will be a difference of two squares.

¹Fragment of a letter of about 1643, Bull. Bibl. Storia Sc. Mat., 12, 1879, 715; Oeuvres de Fermat, 2, 1894, 256. At the time of his letter to Mersenne, Dec. 26, 1638, Oeuvres, 2, p. 177, he had no such method.

²Euler's Algebra, Frankfort, 1796, III, 2. Anhang, 269-283. Cf. Kausler, De Cribro Eratosthenis, 1812.

³Nova Acta Acad. Petrop., 14, ad annos 1797-8 (1805), 268-289.

⁴Bull. Ac. Sc. St. Pétersbourg, 6, 1840, 84-88.

F. Landry⁵ used the method of Fermat, eliminating certain squares by their endings and others by the use of moduli.

C. Henry⁶ stated that Landry's method is merely a perfection of the method given in the article "nombre premier" in the Dictionnaire des Mathématiques of de Montferrier. It is improbable that the latter invented the method (based on the fact that an odd prime is a difference of two squares in a single way), since it was given by Fermat.

F. Thaarup⁷ gave methods to limit the trials for x in $x^2 - y^2 = n$. We may multiply n by $f = a^2 - b^2$ and investigate $nf = X^2 - Y^2$, $X = ax - by$, $Y = bx - ay$. We may test small values of y , or apply a mechanical test based on the last digit of n .

C. J. Busk⁸ gave a method essentially that by Fermat. It was put into general algebraic form by W. H. H. Hudson.⁹ Let N be the given number, n^2 the next higher square. Then

$$N = n^2 - r_0 = (n+1)^2 - r_1 = \dots,$$

where r_1, r_2, \dots are formed from r_0 by successive additions of $2n+1, 2n+3, 2n+5, \dots$. Thus $r_m = r_0 + 2mn + m^2$. If r_m is a square, N is a difference of two squares. A. Cunningham (*ibid.*, p. 559) discussed the conditions under which the method is practical, noting that the labor is prohibitive except in favorable cases such as the examples chosen by Busk.

J. D. Warner^{9a} would make $N = A^2 - B^2$ by use of the final two digits.

A. Cunningham¹⁰ gave the 22 sets of last two digits of perfect squares, as an aid to expressing a number as a difference of two squares, and described the method of Busk, which is facilitated by a table of squares.

F. W. Lawrence¹¹ extended the method of Busk (practical only when the given odd number N is a product of two nearly equal factors) to the case in which the ratio of the factors is approximately l/m , where l and m are small integers. If l and m are both odd, subtract from lmN in turn the squares of $a, a+1, \dots$, where a^2 just exceeds lmN , and see if any remainder is a perfect square (b^2). If so, $lmN = (a+T)^2 - b^2$.

G. Wertheim¹² expressed in general form Fermat's method to factor an odd number m . Let a^2 be the largest square $< m$ and set $m = a^2 + r$. If $\rho \equiv 2a+1-r$ is a square (n^2), we eliminate r and get $m = (a+1+n) \times (a+1-n)$. If ρ is not a square, add to ρ enough terms of the arithmetic progression $2a+3, 2a+5, \dots$ to give a square:

$$\rho + (2a+3) + \dots + (2a+2n-1) = s^2.$$

⁵Aux mathématiciens de toutes les parties du monde: communication sur la décomposition des nombres en leurs facteurs simples, Paris, 1867. Letter from Landry to C. Henry, Bull. Bibl. Storia Sc. Mat., 13, 1880, 469-70.

⁶Assoc. franç. av. sc., 1880, 201; Oeuvres de Fermat, 4, 1912, 208; Sphinx-Oedipe, 4, 1909, 3^e Trimestre, 17-22.

⁷Tidsskrift for Mat., (4), 5, 1881, 77-85.

⁸Nature, 39, 1889, 413-5.

⁹Nature, 39, 1889, p. 510.

^{9a}Proc. Amer. Assoc. Adv. Sc., 39, 1890, 54-7.

¹⁰Mess. Math., 20, 1890-1, 37-45. Cf. Meissner,^{13a} 137-8.

¹¹Ibid., 24, 1894-5, 100.

¹²Zeitschrift Math. Naturw. Unterricht, 27, 1896, 256-7.

Then $2an + n^2 - r = s^2$ and $m = (a + n)^2 - s^2$. The method is the more rapid the smaller the difference of the two factors.

M. Neumann¹³ proved that this process of adding terms leads finally to a square and hence to factors, one of which may be 1.

F. W. Lawrence¹⁴ denoted the sum of the two factors of n by $2a$ and the difference by $2b$, whence $n = a^2 - b^2$. Let q be the remainder obtained by dividing n by a chosen prime p , and write down the pairs of numbers $< p$ such that the product of two of a pair is congruent to q modulo p . If $p = 7$, $q = 3$, the pairs are 1 and 3, 2 and 5, 4 and 6, whence $2a \equiv 4, 0$ or $3 \pmod{7}$. Using various primes p and their powers, we get limitations on a which together determine a . The work may be done with stencils. The method was used by Lawrence¹⁵ to show that five large numbers are primes, including 10, 11 and 12 place factors of $3^{23} - 1$, $10^{29} - 1$, $10^{25} - 1$, respectively. The same examples were treated by other methods by D. Biddle.¹⁶

A. Cunningham¹⁷ remarked that in computing by Busk's method a k for which $(s + k)^2 - N$ is a square, we may use the method of Lawrence, just described, to limit greatly the number of possible forms of k .

F. J. Vaes¹⁸ expressed N in the form $a^2 - b^2$ by use of the square a^2 just $> N$ and then increasing a by 1, 2, . . . , and gave (pp. 501-8) an abbreviation of the method. He strongly recommended the method of remainders (p. 425): If p is a factor of $G = h^2 - g^2$, and if $g = (G - 1)/2$ has the remainder r when divided by p , then $h = (G + 1)/2$ must have the remainder $r + 1$, so that p is a factor of $2r + 1 \equiv G$. For example, let $G = 80047$, whence

$$g = 200^2 + 23 = 201 \cdot 199 + 24 = 202 \cdot 198 + 27, \dots$$

For $r = 24, 27, 32, \dots$ we see that $2r + 1$ is not a multiple of 201, 202, . . . until we reach $g = 209 \cdot 191 + \rho$, $\rho = 104$, $2\rho + 1 = 209$. Thus 209 divides G .

P. F. Teilhet¹⁹ wrote $N = a^2 - b$ in the form $(a + k)^2 - P$, where $P = k^2 + 2ak + b$. Give to k successive values 1, 2, . . . (by additions to P), until P becomes a square v^2 . To abbreviate consider the residues of P for small prime moduli.

E. Lebon²⁰ proceeded as had Teilhet¹⁹ and then set $f = a + k - v$. Then

$$2kf = (a - f)^2 - b,$$

and we examine primes $f < a$ to see if k is an integer.

M. Kraitchik²¹ would express a given odd number A in the form $y^2 - x^2$ by use of various moduli p . Let $A \equiv r \pmod{p}$ and let a_1, \dots, a_n be the

¹³Zeitschrift Math. Naturw. Unterricht, 27, 1896, 493-5; 28, 1897, 248-251.

¹⁴Quar. Jour. Math., 28, 1896, 285-311. French transl., Sphinx-Oedipe, 5, 1910, 98-121, with an addition by Lawrence on $g^{2^k} + 1$.

¹⁵Proc. Lond. Math. Soc., 28, 1897, 465-475. French transl., Sphinx-Oedipe, 5, 1910, 130-6.

¹⁶Math. Quest. Educat. Times, 71, 1899, 113-4; cf. 93-99.

¹⁷Ibid., 69, 1898, 111.

¹⁸Proc. Sect. Sciences Akad. Wetenschappen Amsterdam, 4, 1902, 326-336, 425-436, 501-8 (English); Verslagen Ak. Wet., 10, 1901-2, 374-384, 474-486, 623-631 (Dutch).

¹⁹L'intermédiaire des math., 12, 1905, 201-2. Cf. Sphinx-Oedipe, 1906-7, 49-50, 55.

²⁰Assoc. franç. av. sc., 40, 1911, 8-9.

²¹Sphinx-Oedipe, Nancy, Mai, 1911, numéro spécial, pp. 10-16.

quadratic residues of ρ . Then $r+x^2 \equiv a_i \pmod{\rho}$. Thus a_i-r must be a quadratic residue. Reject from a_1, \dots, a_n the terms for which a_i-r is not in the set. We get the possible residues of x modulo ρ . His method to factor $a^n \neq 1$ is the same as Dickson's¹¹⁸ and is applied to show that the factor $(2^{73}+2^{37}+1)/(5 \cdot 239 \cdot 9929)$ of $2^{146}+1$ is a prime in case it has no factor between 10500 and 108000.

Kraitchik²² extended the method of Lawrence.

F. J. Vaes²³ applied his¹⁸ method to factor Mersenne's¹ number. The same was factored by various methods in *L'Intermédiaire des Mathématiciens*, 19, 1912, 32-5. J. Petersen, *ibid.*, 5, 1898, 214, noted that its product by 8 equals k^2+k , where $k=898423$.

METHOD OF FACTORING BY SUM OF TWO SQUARES.

Frenicle de Bessy²⁵ proposed to Fermat that he factor h given that

$$h = a^2 + b^2 = c^2 + d^2, \quad \text{as } 221 = 100 + 121 = 196 + 25.$$

In 1647, Mersenne⁶¹ (of Ch. I) noted that a number is composite if it be a sum of two squares in two ways.

L. Euler²⁶ noted that N is a prime if it is expressible as a sum of two squares in a single way, while if $N = a^2 + b^2 = c^2 + d^2$, N is composite:

$$N = \frac{\{(a-c)^2 + (b-d)^2\} \{(a+c)^2 + (b+d)^2\}}{4(b-d)^2}.$$

Euler²⁷ proved, that, if a number $N = 4n+1$ is expressible as the sum of two relatively prime squares in a single way, it is a prime. For, if N were composite, then $N = (a^2 + b^2)(c^2 + d^2)$ is the sum of the squares of $ac \pm bd$ and $ad \mp bc$, contrary to hypothesis. If $N = a^2 + b^2 = c^2 + d^2$, N is composite; for if we set $a = c+x$, $d = b+y$, and assume* that the common value of $2cx+x^2$ and $2by+y^2$ is of the form xyz , we get

$$2c = yz - x, \quad 2b = xz - y, \quad N = b^2 + c^2 + xyz = \frac{1}{4}(x^2 + y^2)(1 + z^2),$$

whence $x^2 + y^2$ or $(x^2 + y^2)/4$ is a factor of N . To express N as a sum of two squares in all possible ways, use is made of the final digit of N to limit the squares x^2 to be subtracted in seeking differences $N - x^2$ which are squares. Several numerical examples of factoring are treated in full.

Euler²⁸ gave abbreviations of the work of applying the preceding test. For example, if $4n+1 = 5m+2 = x^2 + y^2$, then x and y are of the form

²²Sphinx-Oedipe, 1912, 61-4.

²³L'enseignement math., 15, 1913, 333-4.

²⁵Oeuvres de Fermat, 2, 1894, 232, Aug. 2, 1641.

²⁶Letters to Goldbach, Feb. 16, 1745, May 6, 1747; Corresp. Math. Phys. (ed., Fuss), I, 1843, 313, 416-9.

²⁷Novi Comm. Ac. Petrop., 4, 1752-3, p. 3; Comm. Arith., 1, 1849, 165-173.

*Euler gave a faultless proof in the margin of his posthumous paper, Tractatus, §570, Comm. Arith., 2, 573; Opera postuma, I, 1862, 73. We have $(a+c)(a-c) = (b+d)(d-b) = pqr$, $a+c=pq$, $a-c=rs$, $b+d=pr$, $d-b=qs$ [since, if p be the g. c. d. of $a+c$, $b+d$, then $q(a-c)$ is divisible by r , whence $a-c=rs$]. Hence $a^2+b^2 = (p^2+s^2)(q^2+r^2)/4$.

²⁸Novi Comm. Ac. Petrop., 13, 1768, 67; Comm. Arith., 1, 379.

$5p \neq 1$. To express a number as $x^2 + y^2$, subtract squares in turn and seek a remainder which is a square.

N. Beguelin²⁹ proposed to find x such that $4p^2x^2 + 1$ is a prime by excluding the values x making the sum composite. The latter is the case if

$$4p^2x^2 + 1 = 4b^2 + (2c + 1)^2, \quad x^2 = \frac{b^2 + c^2 + c}{p^2}.$$

Set $x = q + b/p$. Then b is expressed rationally in terms of c and the known p . Taking $p = 1$, he derived a tentative process for finding a prime, of the form $4x^2 + 1$, which exceeds a given number a .

L. Euler³⁰ proved that $1000^2 + 3^2$ is prime since not expressible as a sum of two squares another way.

A. M. Legendre^{30a} factored numbers represented as a sum of two squares in two ways.

J. P. Kulik's^{30b} tables VIII and IX, relating to the ending of squares, serve to test if $4n + 1$ is a sum of two squares and hence to test if it be prime or composite.

Th. Harmuth³¹ suggested testing $a^2 + b^2$ for factors, where a and b are relatively prime, by noting that it is divisible by 5 if $a \equiv \pm 1$, $b \equiv \pm 2 \pmod{5}$, and similar facts for $p = 13, 17, 29, 37$, there being $p - 1$ sets of values of a, b for each prime $p = 4n + 1$.

G. Wertheim³² explained in full Euler's²⁷ method of factoring.

R. W. D. Christie and A. Cunningham³³ granted $N = A^2 + B^2 = C^2 + D^2$ and showed how to find a, \dots, d so that $N = (a^2 + b^2)(c^2 + d^2)$. Similarly, if $N = x^2 + Py^2$ in two ways.

FACTORING BY USE OF BINARY QUADRATIC FORMS.

L. Euler³⁷ noted that a number is composite if it be expressible in two ways in the form $f = ax^2 + \beta y^2$. The product of two numbers of the form f is of the form $g = a\beta x^2 + y^2$; the product of a number of the form f by one of the form g is of the form f . If for $m > 2$ a composite number mp is expressible in a single way in the form f , there exist an infinitude of composite numbers mq expressible in a single way by f . He called (§34) a number N idoneal (numerus idoneus) if, for $a\beta = N$, every number representable by $f = ax^2 + \beta y^2$ (with ax relatively prime to βy) is a prime, the square of a prime, the double of a prime or a power of 2, so that a number representable by f in a single way is a prime. It suffices to test $N + y^2 < 4N$, y prime to N . He gave (§39, p. 208) the 65 idoneal numbers 1, 2, ..., 1848 less than 10000.

²⁹Nouv. Mém. Acad. Sc. Berlin, 1777, année 1775, 300.

³⁰Nova Acta Petrop., 10, 1792 (1778), 63; Comm. Arith., 2, 243-8.

^{30a}Théorie des nombres, ed. 3, 1830, I, 310. Simplification by Vuibert, Jour. de math. élém., 10, p. 42. Cf. l'intermédiaire des math., 1, 1894, 167, 245; 18, 1911, 256.

^{30b}Tafeln der Quadrat und Kubik Zahlen ... bis hundert Tausend, Leipzig, 1848.

³¹Archiv Math. Phys., 67, 1882, 215-9.

³²Elemente der Zahlentheorie, 1887, 295-9.

³³Math. Quest. Educat. Times, (2), 11, 1907, 52-3, 65-7, 89-90.

³⁷Nova Acta Petrop., 13, 1795-6 (1778), 14; Comm. Arith., 2, 198-214.

Euler³⁸ used the idoneal number 232 to find all values of $a < 300$ for which $232a^2 + 1$ is a prime, by excluding the values of a for which $232a^2 + 1 = 232x^2 + y^2$, $y > 1$.

Euler³⁹ noted that $N = a^2 + \lambda b^2 = x^2 + \lambda y^2$ imply

$$N = \frac{1}{4}(\lambda m^2 + n^2)(\lambda p^2 + q^2), \quad a \pm x = \lambda mp, \, nq; \quad y \pm b = mq, \, np,$$

so that $\lambda p^2 + q^2$, or its half or quarter, is a factor of N . He gave (p. 227) his³⁷ former table of 65 idoneal numbers. Given one representation by $\alpha x^2 + \beta y^2$, where $\alpha\beta$ is idoneal, he sought a second representation. If $N = 4n + 2$ is idoneal, $4N$ is idoneal.

Euler⁴⁰ called $mx^2 + ny^2$ a congruent form if every number representable by it in a single way (with x, y relatively prime) is a prime, the square of a prime, the double of a prime, a power of 2, or the product of a prime by a factor of mn . Then also $mnx^2 + y^2$ is a congruent form and conversely. The product mn is called an idoneal or congruent number. His table of 65 idoneal numbers is reproduced (§18, p. 253). He stated rules for deducing idoneal numbers from given idoneal numbers. He factored numbers expressed in two ways by $\alpha x^2 + \beta y^2$, where $\alpha\beta$ is idoneal, and noted that a composite number may be expressible in a single way in that form if $\alpha\beta$ is not idoneal.

Euler⁴¹ proved that the first five squares are the only square idoneal numbers.

C. F. Kausler⁴² proved Euler's theorem that a prime can be expressed in a single way in the form $mx^2 + ny^2$ if m, n are relatively prime. To find a prime v exceeding a given number, see whether $38x^2 + 5y^2 = v$ has a single set of positive solutions x, y ; or use $1848x^2 + y^2$. As the labor is smaller the larger the idoneal number 38.5 or 1848, it is an interesting question if there be idoneal numbers not in Euler's list of 65. Cf. Cunningham.⁶⁹

Euler⁴³ gave the 65 idoneal numbers n (with 44 a misprint for 45) such that a number representable in a single way by $nx^2 + y^2$ (x, y relatively prime) is a prime. By using $n = 1848$, he found primes exceeding 10 million.

N. Fuss⁴⁴ stated the principles due to Euler.³⁷

E. Waring⁴⁵ stated that a number is a prime if it be expressible in a single way in the form $a^2 + mb^2$ and conversely.

A. M. Legendre⁴⁶ would express the number A to be factored, or one of its multiples kA , in the form $t^2 + au^2$, where a is as small as possible and within the limits of his Tables III-VII of the linear forms of divisors of $t^2 \pm au^2$.

³⁸Nova Acta Petrop., 14, 1797-8 (1778), 3; Comm. Arith., 2, 215-9.

³⁹Ibid., p. 11; Comm. Arith., 2, 220-242. For $\lambda = 2$, Opera postuma, I, 1862, 159.

⁴⁰Ibid., 12, 1794 (1778), 22; Comm. Arith., 2, 249-260.

⁴¹Ibid., 15, ad annos 1799-1802 (1778), 29; Comm. Arith., 2, 261-2.

⁴²Ibid., 156-180.

⁴³Nouv. Mém. Berlin, année 1776, 1779, 337; letter to Beguelin, May, 1778; Comm. Arith., 2, 270-1.

⁴⁴Ibid., 340-6.

⁴⁵Médit. Algebr., ed. 3, 1782, 352.

⁴⁶Théorie des nombres, 1798, pp. 313-320; ed. 2, 1808, pp. 287-292. German transl. by Maser, 1, 329-336. Cf. Sphinx-Oedipe, 1906-7, 51.

Then the divisors of A are included among these linear forms. When \sqrt{kA} is converted into a continued fraction, let $(\sqrt{kA} + I)/D$ be a complete quotient, and p/q the corresponding convergent. Then $\pm D = p^2 - kAq^2$, so that the divisors of A are divisors of $p^2 \mp D$.

C. F. Gauss⁴⁷ stated that the 65 idoneal numbers n of Euler and no other numbers have the two properties that all classes of quadratic forms of determinant $-n$ are ambiguous and that any two forms in the same genus (*Geschlecht*) are both properly and improperly equivalent.

Gauss⁴⁸ gave a method of factoring a number M based on the determination of various small quadratic residues of M .

Gauss⁴⁹ gave a second method of factoring M based on the finding of representations of M by forms $x^2 + D$, where D is idoneal.

F. Minding⁵⁰ gave an exposition of the method of Legendre.⁴⁶

P. L. Tchebychef⁵¹ gave a rapid process to find many forms $x^2 \pm ay^2$ which represent a given number A or a multiple of A . Then a table of the linear forms of the divisors of $x^2 \pm ay^2$ serves to limit the possible factors of A .

Tchebychef⁵² gave theorems on the limits between which lie at least one set of integral solutions of $x^2 - Dy^2 = \pm N$. If there are two sets of solutions within the limits, N is composite. There are given various tests for primality by use of quadratic forms.

C. F. Gauss⁵³ left posthumous tables to facilitate factoring by use of his⁴⁹ second method.

F. Grube⁵⁴ criticized and completed certain of Euler's proofs relating to idoneal numbers, here called Euler numbers. While Gauss⁴⁷ said it is easy to prove Euler's⁴³ criterion for idoneal numbers, Grube could prove only the following modification: Let Ω be the set of numbers $D + n^2 \leq 4D$ in which n is prime to D . According as all or not all numbers of Ω are of the form $q, 2q, q^2, 2^\lambda (q \text{ a prime})$, D is or is not an idoneal number.

E. Lucas⁵⁵ proved that if p is a prime and k is a positive integer, and $p = x^2 + ky^2$, then $p \neq x_1^2 + ky_1^2$ for values x_1, y_1 distinct from $\pm x, \pm y$.

P. Seelhoff⁵⁶ made use of 170 determinants (including the 65 idoneal numbers of Euler and certain others of Legendre), such that every reduced form in the principal genus is of the type $ax^2 + by^2$. To factor N seek among the numbers m of which N is a quadratic residue several values

⁴⁷Disq. Arith., 1801, Art. 303.

⁴⁸Ibid., Arts. 329-332.

⁴⁹Ibid., Arts. 333-4.

⁵⁰Anfangsgründe der Höheren Arith., 1832, 185-7.

⁵¹Theorie der Congruenzen (in Russian), 1849; German transl. by H. Schapira, 1889, Ch. 8, pp. 281-292.

⁵²Jour. de Math., 16, 1851, 257-282; Oeuvres, 1, 73.

⁵³Werke, 2, 1863, 508-9.

⁵⁴Zeitschrift Math. Phys., 19, 1874, 492-519.

⁵⁵Nouv. Corresp. Math., 4, 1878, 36. [Euler.⁴⁷]

⁵⁶Archiv Math. Phys., (2), 2, 1885, 329; (2), 3, 1886, 325; Zeitschrift Math. Phys., 31, 1886, 166, 174, 306; Amer. Jour. Math., 7, 1885, 264; 8, 1886, 26-44.

for which N is representable by $x^2 + my^2$. For example, if $N = 31 \cdot 2^{24} + 1$,

$$N = x^2 + 7 \cdot 19 \cdot 83k^2 = y^2 + 19 \cdot 83l^2 = z^2 - 7r^2.$$

Eliminating $19 \cdot 83$ between the first two, we get $\mu N = w^2 - 7t^2$. This with the third leads to factors of N . In general, when elimination of common factors of the m 's has led to representations of two multiples of N by the same form $x^2 + ny^2$, we may factor N unless it be prime.

H. Weber⁵⁷ computed the class invariants for the 65 determinants of Euler and remarked that there is no known proof of the fact found by induction by Euler and Gauss that there are only 65 determinants such that all classes belonging to the determinant are ambiguous and hence each genus has only one class.

T. Pepin⁵⁸ developed the theory of Gauss'⁵³ posthumous tables and the means of deducing complete tables from the given abridged tables. Pepin⁵⁹ showed how to abridge the calculations in using the auxiliary tables of Gauss in factoring $a^n - 1$, where a and n are primes.

D. F. Seliwanoff⁶⁰ noted that the factoring of numbers of the form $t^2 - Du^2$ reduces to the solution of $(D/x) = 1$, all solutions of which are easily found by use of six relations by Euler on these Jacobi symbols (D/x) .

E. Lucas⁶¹ gave a clear proof of Euler's remark that a prime can not be expressed in two ways in the form $Ax^2 + By^2$, if A, B are positive integers.

S. Levänen⁶² showed and illustrated by examples and tables how binary quadratic forms may be applied to factoring.

G. B. Mathews⁶³ gave an exposition of the subject.

T. Pepin⁶⁴ applied determinants $-8n - 3$ for which each genus has three classes of quadratic forms. The paper is devoted mainly to the solution of $x^2 + (8n + 3)y^2 = 4A$, where A is the number to be factored.

T. Pepin⁶⁵ assumed that the given number N had been tested and found to have no prime factor $\leq p$. Let $\lambda x + 1, \lambda y + 1$ be the two factors of N , each between p and N/p . The sum of the factors lies between $2\sqrt{N}$ and $p + N/p$. Let $x - y = u$, $x + y = \rho z$. Then $(N - 1)/\lambda = \lambda xy + x + y$ gives

$$\frac{4(N - 1)}{\lambda^2} = \rho^2 z^2 + \frac{4\rho}{\lambda} z - u^2,$$

in which special values are assigned to ρ . This equation yields a quadratic congruence for u^2 with respect to an arbitrary prime modulus, used as an excludant. The method applies mainly to numbers $a^\lambda \pm 1$.

E. Cahen⁶⁶ used the linear divisors of $x^2 + Dy^2$.

⁵⁷Math. Annalen, 33, 1889, 390-410.

⁵⁸Atti Accad. Pont. Nuovi Lincei, 48, 1889, 135-156.

⁵⁹*Ibid.*, 49, 1890, 163-191.

⁶⁰Moscow Math. Soc., 15, 1891, 789; St. Petersburg Math. Soc., 12, 1899.

⁶¹Théorie des nombres, 1891, 356-7.

⁶²Öfversigt af finska Vetenskaps-Soc. förhandlingar, 34, 1892, 334-376.

⁶³Theory of Numbers, 1892, 261-271. French transl., Sphinx-Oedipe, 1907-8, 155-8, 161-70.

⁶⁴Memorie Accad. Pontif. Nuovi Lincei, 9, I, 1893, 46-76. Cf. Pepin,⁶⁵ 332.

⁶⁵*Ibid.*, 17, 1900-1, 321-344; Atti, 54, 1901, 89-93. Cf. Meissner¹²³, 121-2.

⁶⁶Éléments de la théorie des nombres, 1900, 324-7. Sphinx-Oedipe, 1907-8, 149-155.

A. Cunningham⁶⁷ and J. Cullen listed the 188 prime numbers $x^2 + 1848y^2$ between 10^7 and $101 \cdot 10^5$, with x prime to $1848y$.

A. Cunningham⁶⁸ noted that two representations of N by $\mu x^k + \nu y^k$ lead to factors of N under certain conditions.

A. Cunningham⁶⁹ recalled that an idoneal number I has the property that, if an odd number N is expressible in only one way in the form $N = mx^2 + ny^2$, where $mn = I$, and mx^2 is prime to ny^2 , then N is a prime or the square of a prime. Euler's largest I is 1848. There is no larger I under 50000, a computation checked by J. Cullen. Cunningham noted on the proof-sheets of this history that this limit has been extended to 100 000.

A. Cunningham⁷⁰ noted conditions that an odd prime be expressible by $t^2 \pm qu^2$ when q or $-q$ is idoneal.

F. N. Cole⁷¹ discussed Seelhoff's⁵⁶ method of factoring.

Al. Laparewicz⁷² described and applied Gauss' ^{48,49} two methods.

P. Meyer⁷³ discussed Euler's theorem that, if n is idoneal, a number representable only once by $x^2 + ny^2$ is a prime.

R. Burgwedel⁷⁴ gave an exposition and completion of the method of Euler³⁷⁻⁴³ and an exposition of the methods of Gauss.^{48,49}

L. Valroff stated and A. Cunningham^{74a} proved that $(Dx^2 - a^2)(Dy^2 - a^2) = Dz^2 - a^2$ implies that one factor is composite unless $x^2 = y^2 = 4$ when $a = 1$, $D = 2$, and in the remaining cases if the two factors are distinct and > 1 .

A. Gérardin⁷⁵ gave a method illustrated for $N = a^2 - 5 \cdot 29^2$, where $a = 6326$. We shall have a second such representation $N = (a + 5x)^2 - 5y^2$ if

$$E \equiv 5x^2 + 2ax + 841 = y^2.$$

Use is made of various moduli $m = 4, 3, 7, 25, \dots$. On square-ruled paper, mark $x = 0, 1, 2, \dots$ at the head of the columns. On the line for modulus m , shade the square under the heading x when x makes E a quadratic non-residue of m . Then examine the column in which occurs no shaded square. Up to $x \leq 15$, these are $x = 0$ (excluded), and $x = 4$, which gives $N = 6346^2 - 5 \cdot 227^2$ and the factor $99^2 - 5 \cdot 2^2$. The same diagram serves for all numbers $1050H + 671$, our N being given by $H = 38108$. To apply the method to $N = (2x)^4 + 1 = (4x^2 + 1)^2 - 2(2x)^2$, seek a second representation $N = (4x^2 + 2p + 1)^2 - 2(2u)^2$. The condition is $(2p + 1)x^2 + \frac{1}{2}p(p + 1) = u^2$, solutions of which are found for $p = 1, 8, 9, \dots, 6^2, 35^2, \dots$. Or we may choose x , say $x = 48$, and find $p = 8$, $u = 198$.

⁶⁷Brit. Assoc. Reports, 1901, 552. The entry 10098201 is erroneous.

⁶⁸Proc. London Math. Soc., 33, 1900-1, 361.

⁶⁹*Ibid.*, 34, 1901-2, 54.

⁷⁰*Ibid.*, (2), 1, 1903, 134.

⁷¹Bull. Amer. Math. Soc., 10, 1903-4, 134-7.

⁷²Prace mat. fiz., Warsaw, 16, 1905, 45-70 (Polish).

⁷³Beweis eines von Euler entdeckten Satzes, betreffend die Bestimmung von Primzahlen, Diss., Strassburg, 1906.

⁷⁴Ueber die Eulerschen und Gausschen Methoden der Primzahlbestimmung, Diss., Strassburg, 1910, 101 pp.

^{74a}Sphinx-Oedipe, 7, 1912, 60, 77-9.

⁷⁵Wiskundig Tijdschrift, 10, 1913, 52-62.

Gérardin⁷⁶ gave a note on his machine to factor large numbers, especially those of the form $2x^4 - 1$.

FACTORING BY METHOD OF FINAL DIGITS.

Johann Tessanek⁸⁰ gave a tedious method of factoring N , not divisible by 2, 3, or 5, when $N/10$ is within the limits of a factor table. For example, let $N = 10a + 1$; its factors end in 1, 1 or 3, 7 or 9, 9. To treat one of the four cases, consider a factor $10x + 3$, the quotient being $10z + 7$. Then z is the quotient of $a - 2 - 7x$ by $10x + 3$. Give to x the values 1, 2, . . . , and test $a - 9$ for the factor 13, $a - 16$ for 23, etc., by the factor table. He gave a lengthy extension⁸¹ to divisors $100x + 10f + g$. Again, to factor $N = 2a + 1$, given a table extending to $N/2$, note that if $2x + 1$ is a divisor of N , it divides $a - x$, which falls in the table. F. J. Studnicka⁸² quoted the last result.

N. Beguelin⁸³ would factor $N = 4p + 3$ by considering the final digit of $\pi = (N - 11)/4$ and hence find the proper line in an auxiliary table (pp. 291-2), each line containing four fractional expressions. Proceed with each until we reach a fraction whose numerator is zero. Then its denominator is a factor of N .

Georg Simon Klügel⁸⁴ noted that a number, not divisible by 2, 3 or 5, is of the form $30x + m$ ($m = 1, 7, 11, 13, 17, 19, 23, 29$). Suppose $10007 = (30x + m)(30y + n)$. Then $(m, n) = (1, 17), (7, 11), (13, 29)$ or $(19, 23)$. For $m = 1, n = 17$, we get

$$x = \frac{333 - y}{30y + 17}, \quad x < 4, y < 4.$$

But x is not integral for $y = 0, 1, 2, 3$.

Johann Andreas von Segner (*ibid.*, 217-225) took two pages to prove that any number not divisible by 2 or 3 is of the form $6n \pm 1$ and noted that, given a table of the least prime factor of each $6n \pm 1$, he could factor any number within the limits of the table!

Sebastiano Canterzani⁸⁵ would factor $10k + 1$, by noting the last digits 1, 1 or 3, 7 or 9, 9 of its factors. If one factor ends in 7, there are 10 possibilities for the digit preceding 7; if one ends in 1 or 9, there are five cases; hence 20 cases in all. A. Niegemann^{85a} used the same method.

Anton Niegemann⁸⁶ gave a method of computing a table of squares arranged according to the last two digits. Thus, if $A76 = (10x - 6)^2$, then

⁷⁶Assoc. franç. avanc. sc., 43, 1914, 26-8. Proc. Fifth Internat. Congress, II, 1913, 572-3; Brit. Assoc. Reports, 1912-3, 405.

⁸⁰Abhandl. einer Privatgesellschaft in Böhmen, zur Aufnahme der Math., Geschichte, . . . , Prag, I, 1775, 1-64.

⁸¹M. Cantor, Geschichte Math., 4, 1908, 179.

⁸²Casopis, 14, 1885, 120 (Fortschr. der Math., 17, 1885, 125).

⁸³Nouv. Mém. Ac. Berlin, année 1777 (1779), 265-310.

⁸⁴Leipziger Magazin für reine u. angewandte Math. (eds., J. Bernoulli und Hindenburg), 1, 1787, 199-216.

⁸⁵Memorie dell' Istituto Nazionale Italiano, Classe di Fis. e Mat., Bologna, 2, 1810, II, 445-476.

^{85a}Entwicklung . . . Theilbarkeit, Jahresber. Kath. Gymn. Köln., 1847-8, 23.

⁸⁶Archiv Math. Phys., 45, 1866, 203-216.

$A0 = 10x^2 - 12x - 4$, whence $12x + 4$ is divisible by 10, so that $x = 5d - 2$. Then $A = 25d^2 - 26d + 6$. Thus if we delete the last two digits 7, 6 of squares $A76$, we obtain numbers A whose values for $d = 1, 2, \dots$ can be derived from the initial one 5 by successive additions of 49, $49 + 50$, $49 + 2 \cdot 50, \dots$. He gave such results for every pair of possible endings of squares.

A similar method is applied to any composite number. One case is when the last two digits are $m, 1$ and $Am1 = (10x - 1)(10y - 1)$. Then

$$A0 = 10xy - y - x - m, \quad y + x + m = 10a, \quad A = 10ax - x^2 - mx - a.$$

The discriminant of the last equation must be a square. A table of values of A for each a may be formed by successive additions.

G. Speckmann⁸⁷ noted that the two factors of $N = 2047$ end in 1 and 7 or 3 and 9. Treating the first case, we see that, if a and b are the digits in tens place, $b + 7a \equiv 4 \pmod{10}$, so that the factors end in 01 and 47, or 11 and 77, etc.

G. Speckmann⁸⁸ wrote the given number prime to 3 in the form $9a + b$ ($b < 9$), so that the sum of its digits is $\equiv b \pmod{9}$. By use of a small auxiliary table we have the residues modulo 9 of the sums of the digits of every possible pair of factors.

R. W. D. Christie⁸⁹ and D. Biddle⁹⁰ made an extensive use of terminal digits.

E. Barbette⁹¹ noted that $10d + u$ has a divisor $10m - 1$ if and only if $d + mu$ has that divisor. Set $d + mu = n(10m - 1)$, $d = 10d' + u'$. Then

$$mn = d' + x, \quad 10x = mu + n + u'.$$

Eliminating n , we get a quadratic for m . Its discriminant is a quadratic function of x which is to be made a square. Similarly for $10m + 1$, $10m \pm 3$.

A. Gérardin^{91a} developed Barbette's⁹¹ method.

R. Rawson⁹² found Fermat's¹ factors of a number proposed by Mersenne by writing it to the base 100 and expressing it as $(a \cdot 10^2 + 23)(b \cdot 10^2 + 3)$.

J. Deschamps⁹³ would use the final digits and auxiliary tables.

A. Gérardin⁹⁴ would factor N (prime to 2, 3, 5) by use of

$$N = 120n + K = (120x + a)(120y + b),$$

and a table showing, for each of the 32 values of $K < 120$, the 16 pairs a, b (each < 120) such that $ab \equiv K \pmod{120}$. He factored Mersenne's number.¹

FACTORING BY CONTINUED FRACTIONS OR PELL EQUATIONS.

Franz von Schaffgotsch¹⁰⁰ would factor a by solving $az^2 + 1 = x^2$ (having

⁸⁷Archiv Math. Phys., (2), 12, 1894, 435.

⁸⁸Archiv. Math. Phys., 14, 1896, 441-3.

⁸⁹Math. Quest. Educat. Times, 69, 1898, 99-104. Cf. Meissner,¹³⁸ 138-9.

⁹⁰*Ibid.*, 87-88, 112-4; 71, 1899, 93-9; Mess. Math., 28, 1898-9, 120-149, 192 (correction). Cf. Meissner,¹³⁸ 137-8.

⁹¹Mathesis, (2), 9, 1899, 241.

^{91a}Sphinx-Oedipe, 1906-7, [1-2, 17, 33], 49-50, 54, 65-7, 77-8, 81-4; 1907-8, 33-5; 5, 1910, 145-7; 6, 1911, 157-8.

⁹²Math. Quest. Educat. Times, 71, 1899, 123-4.

⁹³Bull. Soc. Philomathique de Paris, (9), 10, 1908, 10-26.

⁹⁴Assoc. franç., 38, 1909, 145-156; Sphinx-Oedipe, Nancy, 1908-9, 129-134, 145-9; 4, 1909, 3^e Trimestre, 17-25.

¹⁰⁰Abh. Böhmischen Gesell. Wiss., Prag, 2, 1786, 140-7.

solutions if a is not a square) and testing $x^2 - 1$ for a factor in common with a . Further, if $ay + 1 = x^2$ does not hold for $1 < x < a - 1$, then a is a power of a prime and conversely [false if $a = 10$].

Märcker¹⁰¹ noted that if there are $2n$ terms in the period of

$$\sqrt{A} = a + \frac{1}{a'} + \frac{1}{a''} + \dots$$

and $Q = 0$, $Q' = a$, $Q'' = a'P' - Q'$, \dots ,

$$P = 1, \quad P' = \frac{A - Q'^2}{P}, \quad P'' = \frac{A - Q''^2}{P'}, \dots,$$

then the n th P or its half is a factor of A . If A is a prime, then the n th P is 2.

J. G. Birch¹⁰² derived a factor of N from a solution x of $x^2 = Ny + 1$. The continued fraction for $x/(N - x)$ is of the form

$$\frac{1}{a_0 - 1} + \frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_2} + \frac{1}{a_1} + \frac{1}{a_0},$$

and N is the continuant defined as the determinant with $a_0, a_1, \dots, a_{n-1}, a_n, a_{n-1}, \dots, a_1, a_0$ in the main diagonal, elements $+1$ just above this diagonal, elements -1 just below, and zeros elsewhere. Then the continuant with the diagonal a_0, \dots, a_{n-1} is a factor of N .

W. W. R. Ball¹⁰³ applied this method to a number of Mersenne.¹

A. Cunningham¹⁰⁴ noted that a set of solutions of $y^2 - Dx^2 = -1$ gives at sight factors of $y^2 + 1$.

M. V. Thielmann¹⁰⁵ illustrated his method by factoring $k = 36343817$. The partial denominators in the continued fraction for \sqrt{k} are 1, 1, 2, 1, 1, 12056. Drop the last term and pass to the ordinary fraction $7/12$. Hence set $(12x + 7)^2 = 12^2y + 1$. The least solution is $x = 4, y = 21$. Using the part of the period preceding the middle term $w = 2$, we get

$$\frac{1}{1+1} = \frac{P}{M}, \quad P = 1, \quad M = 2, \quad Q = wM + 2P = 6, \quad u = MQ = 12.$$

Hence $t^2 - 21u^2 = 1$ has the solution $t = 55$. For a suitably chosen n ,

$$k = u^2n^2 + 2tn + 21 = \left(2q^2n + \frac{t \pm 1}{8}\right) \left(2M^2n + \frac{t \mp 1}{2q^2}\right),$$

where q is the largest integer $\leq Q/2$. Here $n = 502$ and the factors of k are $2 \cdot 3^2n + 7$ and $2 \cdot 2^2n + 3$.

D. N. Lehmer¹⁰⁶ noted that if $R = pq$ is a product of two odd factors whose difference is $< 2\sqrt[4]{R}$, so that $\frac{1}{4}(p - q)^2 < \sqrt{R}$, then

$$x^2 - Ry^2 = \frac{1}{4}(p - q)^2$$

has the integral solutions $x = (p + q)/2, y = 1$. Hence $\frac{1}{4}(p - q)^2$ is a denominator of a complete quotient in the expansion of \sqrt{R} as a continued fraction,

¹⁰¹Jour. für Math., 20, 1840, 355-9. Cf. l'intermédiaire des math., 20, 1913, 27-8.

¹⁰²Mess. Math., 22, 1892-3, 52-5.

¹⁰³Ibid., p. 82-3. French transl., with Birch¹⁰², Sphinx-Oedipe, 1913, 86-9.

¹⁰⁴Ibid., 35, 1905-6, 166-185; abst. in Proc. London Math. Soc., 3, 1905, xxii.

¹⁰⁵Math. Annalen, 62, 1906, 401.

¹⁰⁶Bull. Amer. Math. Soc., 13, 1906-7, 501-2. French transl., Sphinx-Oedipe, 6, 1911, 138-9.

in view of the theorem of Lagrange: If $x^2 - Ry^2 = \pm D$ has relatively prime integral solutions x, y , where $D < \sqrt{R}$, then D is a denominator of a complete quotient in the expansion of \sqrt{R} as a continued fraction.

FACTORING BY USE OF VARIOUS MODULI.

C. F. Gauss¹¹⁰ gave a "method of exclusion," based on the use of various small moduli, to express a given number in a given form $mx^2 + ny^2$.

V. Bouniakowsky¹¹¹ noted that information as to the prime factors of a number N may be obtained by comparing the solution $x = \phi(N)$ of $2^x \equiv 1 \pmod{N}$ with the least positive solution $x = a$ found by a direct process such as the following: Since $2^a = NK + 1$, multiply the given N by the unknown K , each expressed in the binary scale (base 2), add 1 and equate the result to $10 \dots 0$. The digits of K are found seriatim and very simply.

H. J. Woodall¹¹² expressed the number N to be factored in the form $\alpha^a + \beta^b + \dots + r$, where $r < 1000$, while α, β, \dots are small, but not necessarily distinct. Hence the residues of N with respect to various moduli are readily found by tables of residues.

F. Landry¹¹³ employed the method of exclusion by small moduli.

D. Biddle¹¹⁴ investigated factors $2\Delta p + 1$ by using moduli $\Delta^2, 4\Delta^2$.

C. E. Bickmore, A. Cunningham and J. Cullen¹¹⁵ each treated the large factor of $10^{25} + 1$ by use of various moduli, and proved it is prime.

J. Cullen^{115a} gave an effective graphical process to factor numbers by the use of various moduli; the numbers to be searched for in a diagram are all small.

Alfred Johnsen¹¹⁶ used $R_t(p)$ to denote the numerically least residue of p modulo t . Then, for every p, t, k ,

$$[R_t(k)]^2 + R_t(p - k^2) \equiv R_t(p) \pmod{t}.$$

If t is a factor of the given number p , the left member will be divisible by t . In practice take k^2 to be the nearest square to p , larger or smaller. For example, let $p = 4699$, $k^2 = 4624 = 68^2$, $p - k^2 = 75$. Then

t	$[R_t(68)]^2$	$R_t(75)$	Sum
7	4	-2	2
13	9	-3	6
...
37	36	1	37

Thus 37 is the least factor of p .

¹¹⁰Disq. Arith., 1801, Arts. 323-6.

¹¹¹Mém. Ac. Sc. St. Pétersbourg, Math.-Phys., (6), 2, 1841, 447-69. Extract in Bull. Ac. Sc., 6, p. 97. Cf. Nordlund.¹¹⁷

¹¹²Math. Quest. Educat. Times, 70, 1899, 68-71; 71, 1899, 124.

¹¹³Procédés nouveaux..., Paris, 1859. Cf. A. Aubry,¹⁴⁷ pp. 214-7.

¹¹⁴Mess. Math., 30, 1900-1, 98, 190. Math. Quest. Educat. Times, 74, 1901, 147-152.

¹¹⁵Math. Quest. Educat. Times, 72, 1900, 99-103.

^{115a}Ibid., 73, 1900, 133-5; 75, 1901, 102-4. Proc. London Math. Soc., 34, 1901-2, 323-334; (2), 2, 1905, 138-141.

¹¹⁶Nyt Tidsskrift for Mat., 15 A, 1904, 109-110.

K. P. Nordlund¹¹⁷ would use the exponent e to which 2 belongs modulo N [Bouniakowsky¹¹¹]. For $N=91$, $e=12$ is not a divisor of $N-1$, so that N is composite, and we expect the factor 13.

L. E. Dickson¹¹⁸ found the factors of $56^7 \pm 1$, $26^{13} + 1$, $34^{17} + 1$, $52^{13} + 1$ by an expeditious method. For example, each factor of

$$b = \frac{56^7 - 1}{56 - 1} = 1 + 56N$$

is $\equiv 1 \pmod{14}$. Let $b = (1 + 14k)(1 + 14k_1)$. Then

$$k + k_1 + 14kk_1 = 4N, \quad k + k_1 = 4 + 14h.$$

Thus k and k_1 are the roots of a quadratic whose discriminant Q is of the second degree in h . By use of various moduli which are powers of small primes, the form of h is limited step by step, until finally at most a half dozen values of h remain to be tested directly.

L. E. Dickson¹¹⁹ gave further illustrations of the last method.

J. Schatunovsky¹²⁰ reduced to a minimum the number of trials in Gauss'¹¹⁰ method of exclusion, taking the simplest case $m=1$. He gave theorems on the linear forms of the factors of $a^2 + Db^2$, which lead easily to all its odd factors when D is an odd prime.

H. C. Pocklington¹²¹ would use Fermat's theorem to tell whether N is prime or composite. Choose an integer x and find the least positive residue of x^{N-1} modulo N ; if $\neq 1$, N is composite. But if it be unity, let p be a prime factor (preferably the largest) of $N-1$ and contained a times in it. Find the remainder r when x^m is divided by N , where $m = (N-1)/p$. If $r \neq 1$, let δ be the g. c. d. of $r-1$ and N . If $\delta > 1$, we have a factor of N . If $\delta = 1$, all prime factors of N are of the form $kp^a + 1$. But if $r = 1$, replace m by m/q , where q is any prime factor of m and proceed as before.

D. Biddle^{121a} made use of various small moduli.

A. Gérardin^{121b} used various moduli to factor 77073877.

See papers 14, 15, 21, 22, 48, 65.

FACTORIZING INTO TWO NUMBERS $6n \pm 1$.

G. W. Kraft¹²² noted that $6a + 1 = (6m + 1)(6n + 1)$ implies

$$n = \frac{a - m}{6m + 1}.$$

Find which $m = 1, 2, 3, \dots$ makes n an integer.

Ed. Bartl¹²³ tested $6 \cdot 186 + 5$ for a prime factor less than 31, just less than its square root, by noting that 186, 185, 184, 183, 182 are not divisible by 5, 11, 17, 23, 29, respectively; while the last of 7, 13, 19 is a factor.

¹¹⁷Göteborgs Kungl. Vetenskaps. Handl., (4), 1905, VII-VIII, pp. 21-4.

¹¹⁸Amer. Math. Monthly, 15, 1908, 217-222.

¹¹⁹Quar. Jour. Math., 40, 1909, 40-43.

¹²⁰Der Grösste Gemeinschaftliche Teiler von Algebr. Zahlen zweiter Ordnung, Diss. Strassburg, Leipzig, 1912.

¹²¹Proc. Cambridge Phil. Soc., 18, 1914-5, 29-30.

^{121a}Math. Quest. Educat. Times, (2), 25, 1914, 43-6.

^{121b}L'enseignement math., 17, 1915, 244-5.

¹²²Novi Comm. Ac. Petrop., 3, ad annos 1750-1, 117-8.

¹²³Zur Theorie der Primzahlen, Progr. Mies, Pilsen, 1871.

F. Landry¹²⁴ treated the possible pairs $6n \pm 1$ and $6n' \pm 1$ of factors of N . Taking for example the case of the upper signs, we have

$$6nn' + n + n' = \frac{N-1}{6} = 6q + r.$$

Set $n + n' = 6h + r$. Then $nn' = q - h$, whence

$$h = \frac{q - n'(r - n')}{6n' + 1}.$$

Give to n' values such that $6n' + 1$ is a prime $< \sqrt{N}$.

K. P. Nordlund¹²⁵ treated $6p - 1 = (6m + 1)(6n - 1)$ solved for m .

D. Biddle¹²⁶ applied the method to $6n \pm 1$.

Hansen,⁹⁹ of Ch. XIII, used this method.

MISCELLANEOUS METHODS OF FACTORING.

Matsunaga¹²⁹ wrote the number to be factored in the form $r^2 + R$. For r odd, set $r = B_1$, $B_1 - 2 = B_2$, $B_2 - 2 = B_3, \dots$ and perform the following calculations:

$$\begin{array}{lll} R = Q_1 B_1 + A_1, & K_1 = 2Q_1, & K_2' = K_1 + 4, \\ A_1 + K_2' = Q_2 B_2 + A_2, & K_2 = 2Q_2 + K_2', & K_3' = K_2 + 8, \\ A_2 + K_3' = Q_3 B_3 + A_3, & K_3 = 2Q_3 + K_3', & K_4' = K_3 + 8, \end{array}$$

etc., until we reach $A_n = 0$; then B_n is a factor. If r is even, set $r - 1 = B_1$ and replace R by $R + 1$ in what precedes.

J. H. Lambert¹³⁰ used periodic decimals [see Lambert,⁶ Ch. VI].

Jean Bernoulli¹³¹ gave a method based on that of Lambert (*Mém. de Math. Allemands*, vol. 2). Let $A = a^2 + b$ have the factors $a - x$ and $a + x + y$. Then $x^2 = ay - xy - b$. Solve for x . Thus $y^2 + 4ay - 4b$ must be a square. Take $y = 1, 2, \dots$ and use a table of squares.

J. Gough¹³² gave a method to find the factors r, s of each number $f^2 - c$ between $(f-1)^2$ and f^2 . For example, let $f = 3$ and make a double row for each $r = 1, \dots, f$. In the upper row for $r = 1$, insert $2f - 1, \dots, 1, 0$; in the lower, $(f-1)^2, \dots, f^2$. In the upper row for $r = 2$, insert 1 (the remainder

$r = 1$	$c = 5$ $s = 4$	4 5	3 6	2 7	1 8	0 9
$r = 2$	$c = 5$ $s = 2$		3 3		1 4	
$r = 3$	$c =$ $s =$					0 3

¹²⁴Assoc. franç. avanc. sc., 9, 1880, 185-9.

¹²⁵Nyt Tidsskrift for Mat., Kjobenhavn, 15 A, 1904, 36-40.

¹²⁶Math. Quest. Educ. Times, 69, 1898, 87-8; (2), 22, 1912, 38-9, 84-6.

¹²⁹Japanese manuscript, first half eighteenth century, Abhandl. Geschichte Math. Wiss., 30, 1912, 236-7.

¹³⁰Nova Acta Eruditorum, 1769, 107-128.

¹³¹Nouv. Mém. Ac. Berlin, année 1771, 1773, 323.

¹³²Jour. Nat. Phil. Chem. Arts (ed., Nicholson), 1, 1809, 1-4.

on dividing f^2 by 2), 1+2, 1+2+2 under 1, 3, 5 of the first row for $r=1$; in the lower row, insert 4 (the quotient), 4-1, 4-2. To factor f^2-c , locate the column headed by the given c ; thus, for $c=3$, the factors are $s=6$, $r=1$ and $s=3$, $r=2$. Since $c=2$ occurs only in the first row, 9-2 is prime.

Joubin,¹³³ J. P. Kulik,¹³⁴ O. V. Kielsen,¹³⁵ and G. K. Winter¹³⁶ published papers not accessible to the author.

E. Lucas gave methods of factoring and tests for primes (Ch. XVII).

D. Biddle¹³⁷ wrote the proposed number N in the form S^2+A , where S^2 is the largest square $<N$. Write three rows of numbers, the first beginning with A , or $A-S$ if $A>S$; the second beginning with S (or $S+1$) and increasing by 1; the third beginning with S and decreasing by 1. Let A_n , B_n , C_n be the n th elements in the respective rows. Then

$$C_n = C_{n-1} - 1, \quad B_n = B_{n-1} + 1, \quad A_n = A_{n-1} + B_{n-1} - C_n,$$

except that, when $A_n > C_n$, we subtract C_n from A_n as often (say k times) as will leave a positive remainder, and then $B_n = B_{n-1} + 1 + k$. When we reach a value of n for which $A_n = 0$, we have $N = B_n C_n$. For example, if $N = 589 = 24^2 + 13$, the rows are

13	14	17	1	9	0	
24	25	26	28	29	31	(factors 31, 19).
24	23	22	21	20	19	

It may prove best to start with $2N$ instead of with N .

O. Meissner¹³⁸ reviewed many methods of factoring.

R. W. D. Christie¹³⁹ gave an obscure method by use of "roots."

Christie¹⁴⁰ noted that, if $N = AB$,

$$A = (4bN + d^2 - d)/(2b), \quad B = (4bN + d^2 + d)/2, \quad d \equiv a - bc,$$

whence $d^2 = (B - bA)^2$.

D. Biddle¹⁴¹ gave a method of finding the factors of N given those of $N+1$. Set $L = N-1$. Try to choose K and M so that $KM = N+1$ and so that $1+K$ is a factor of N . Since $2N = (1+K)M + L - M$, we will have $L - M = (1+K)m$, whence $2N = (1+K)(M+m)$. For $N = 1829$, $N+1 = 2 \cdot 3 \cdot 5 \cdot 61$. Take $K = 30$, $M = 61$. Then $m = 57$, $M+m = 2 \cdot 59$, $N = 31 \cdot 59$. He gave (*ibid.*, p. 43) the theoretical test that $N = S^2 + A$ is composite if the sum of r terms of

$$\frac{A}{S} + \frac{N}{S(S-1)} + \frac{N}{(S-1)(S-2)} + \dots$$

is an integer for some value of r .

¹³³Sur les facteurs numériques, Havre, 1831.

¹³⁴Abh. K. Böhm. Gesell. Wiss., 1, 1841 (2, 1842-3, 47, graphical determination of primes).

¹³⁵Om et heel tals upplösning i factorer, Kjöbenhavn, 1841.

¹³⁶Madras Jour. Lit. Sc., 1886-7, 13.

¹³⁷Mess. Math., 28, 1898-9, 116-20; Math. Quest. Educat. Times, 70, 1899, 100, 122; 75, 1901, 48; extension, (2), 29, 1916, 43-6.

¹³⁸Math. Naturw. Blätter, 3, 1906, 97, 117, 137.

¹³⁹Math. Quest. Educat. Times, (2), 12, 1907, 90-1, 107-8.

¹⁴⁰*Ibid.*, (2), 13, 1908, 42-3, 62-3.

¹⁴¹*Ibid.*, (2), 14, 1908, 34. The process is well adapted to factoring $2^p - 1$, (2), 23, 1913, 27-8.

E. Lebon^{141a} would first test N for prime factors P just $< \sqrt{N}$. Let Q be the quotient and R the remainder on dividing N by P . If Q and R have a common factor, it divides N ; if not, N is not divisible by any factor of Q or of R .

D. Biddle¹⁴² considered $N = S^2 + A = (S+u)(S-v)$, wrote $uv = N_1$ and obtained like equations in letters with subscripts unity. Then treat $u_1v_1 = N_2$ similarly, etc.

A. Cunningham¹⁴³ noted that the number of steps in Biddle's¹⁴² process is approximately the value of k in $2^k = N$, and developed the process.

E. Lebon¹⁴⁴ treated the decomposition of forms

$$x^a \pm x^b \pm x^c \pm \dots \pm 1 \quad (\alpha > \beta > \gamma \dots)$$

of degrees ≤ 9 into two such forms, using a table of those forms of degrees ≤ 4 with all coefficients positive which are not factorable. The base most used in the examples is $x = 10$. But bases 2 and 3 are considered.

E. Barbette¹⁴⁵ quoted from his¹⁴⁶ text the theorem that any integer N can be expressed in each of the four forms

$$N = \Delta_x - \Delta_y, \quad 8N = x^2 - y^2, \quad Nz = \Delta_x, \quad 8Nz + 1 = y^2,$$

where $\Delta_x = x(x+1)/2$. The resulting new methods of factoring are now simplified by use of triangular and quadratic residues. The first formula implies $N = (x-y)(x+y+1)/2$. In his text, he considered the sum

$$N = (y+1) + (y+2) + \dots + (x-1) + x = \Delta_x - \Delta_y$$

of consecutive integers. Treating four types of numbers N , he proved that this equation has 1, 2 or more than 2 sets of integral solutions x, y , according as N is a power of 2, an odd prime, or a composite number not a power of 2. He proved independently, but again by use of sums of consecutive integers, that every composite number not a power of 2 can be given the form* $N = u(2v-u+1)/2$, where u and v are integers and $v \geq u \geq 3$. Solving for u , and setting $x = 2v+1$, we get $2u = x + (x^2 - 8N)^{1/2}$. Hence $x^2 - 8N = y^2$ is solvable in integers [evidently by $x = 2N+1$, $y = 2N-1$]. Finally, $Nz = \Delta_x$ is equivalent to $(2x+1)^2 = 8Nz+1$. For four types of numbers N , the solutions of $y^2 = 8Nz+1$ are found and seen to involve at least two arbitrary constants.

A. Aubry¹⁴⁷ reviewed various methods of factoring.

^{141a}Il Pitagora, Palermo, 14, 1907-8, 96-7.

¹⁴²Math. Quest. Educat. Times, (2), 19, 1911, 99-100; 22, 1912, 38-9; Educat. Times, 63, 1910, 500; Math. Quest. and Solutions, 2, 1916, 36-42.

¹⁴³Ibid., (2), 20, 1911, 59-64; Educat. Times, 64, 1911, 135.

¹⁴⁴Bull. soc. philomathique de Paris, (10), 2, 1910, 45-53; Sphinx-Oedipe, 1908-9, 81-3, 97-101

¹⁴⁵L'enseignement math., 13, 1911, 261-277.

¹⁴⁶Les sommes de p -ièmes puissances distinctes égales à une p -ième puissance, Paris, 1910, 20-76.

*This follows from the former result $N = (x-y)(x+y+1)/2$ by setting $x = v$, $y = v-u$. To give a direct proof, take u to be the least odd factor > 1 of the composite number N not a power of 2; then $q = N/u$ can be given the form $v - (u-1)/2$ by choice of v . If $v < u$, then $q < (u+1)/2 < u$, so that q has no odd factor and $q = 2^h$. But $N = 2^h u$ is of the desired form if we take $v = u/2 = N$.

¹⁴⁷Sphinx-Oedipe, numéro spéc., June, 1911, 1-27. Errata and addenda, numéro spéc., Jan., 1912, 7-9, 14. L'enseignement math., 15, 1913, 202-231.

S. Bisman¹⁴⁸ noted that N is composite if and only if there exist two integers A, B such that $A+2B$ and $A+2BN$ divide $2(N-1)$ and $(N-1)A$, respectively. But there is no convenient maximum for the smaller integer B . To find the factor 641 of $2^{32}+1$ there are 16 cases.

A. Gérardin¹⁴⁹ gave a report on methods of factoring.

J. A. Gmeiner,¹⁵⁰ to factor a , prime to 6, determined b and ϵ so that $9a=16b+\epsilon$, $0\leq\epsilon<16$. Let ω^2 be the largest square $<b$ and set $b=\omega^2+\rho$, $\sigma=\rho-\omega$. Hence $9a=16(\omega-x)(\omega+x+1)+\tau(x)$, where

$$\tau(x)=16\sigma+\epsilon+16x(x+1).$$

Since $\tau(x)=\tau(x-1)+32x$, we may rapidly tabulate the values of $\tau(x)$ for $x=0, 1, 2, \dots$. If we reach the value zero, we have two factors of a . To prove that a is a prime, we need extend the table until $\omega+x+1$ is the largest square $<a$. To modify the process, use $4a=7b+\epsilon$.

A. Reymond¹⁵¹ used the graphs of $y=x/n$ ($n=1, 2, 3, 5, \dots$), marking on each the points with integral coordinates. He omitted $y=x/4$ since its integral points are on $y=x/2$. Since 17 is not the abscissa of an integral point on $y=x/n$ for $1<n<17$, 17 is a prime. [Möbius^{53a} of Ch. XIII.]

A. J. Kempner¹⁵² found, by use of a figure perspective to Reymond's¹⁵¹, how to test the primality of numbers by means of the straight edge.

D. Biddle and A. Cunningham¹⁵³ factor a product N of two primes by finding $N_1<N$ and $N_2>N$ such that $N_2-N=N-N_1+2$, while each of N_1 and N_2 is a product of two even factors, the two smaller factors differing by 2 and the two larger factors differing by 2.

¹⁴⁸Mathesis, (4), 2, 1912, 58-60.

¹⁴⁹Assoc. franç. avanc. sc., 41, 1912, 54-7.

¹⁵⁰Monatshefte Math. Phys., 24, 1913, 3-26.

¹⁵¹L'enseignement math., 18, 1916, 332-5.

¹⁵²Amer. Math. Monthly, 24, 1917, 317-321.

¹⁵³Math. Quest. and Solutions, 3, 1917, 21-23.

CHAPTER XV.

FERMAT NUMBERS $F_n = 2^{2^n} + 1$.

Fermat¹ expressed his belief that every F_n is a prime, but admitted that he had no proof. Elsewhere² he said that he regarded the theorem as certain. Later³ he implied that it may be proved by "descent." It appears that Frenicle de Bessy confirmed this conjectured theorem of Fermat's. On several occasions Fermat⁴ requested Frenicle to divulge his proof, promising important applications. In the last letter cited, Fermat raised the question if $(2k)^{2^m} + 1$ is always a prime except when divisible by an F_n .

C. F. Gauss⁵ stated that Fermat affirmed (incorrectly) that the theorem is true. The opposite view was expressed by P. Mansion⁶ and R. Baltzer.⁷

F. M. Mersenne⁸ stated that every F_n is a prime. Chr. Goldbach⁹ called Euler's attention to Fermat's conjecture that F_n is always prime, and remarked that no F_n has a factor < 100 ; no two F_n have a common factor.

L. Euler¹⁰ found that

$$F_5 = 2^{32} + 1 = 641 \cdot 6700417.$$

Euler¹¹ proved that if a and b are relatively prime, every factor of $a^{2^n} + b^{2^n}$ is 2 or of the form $2^{n+1}k + 1$ and noted that consequently any factor of F_5 has the form $64k + 1$, $k = 10$ giving the factor 641.

Euler^{11a} and N. Beguelin¹² used the binary scale to find the factor $641 = 1 + 2^7 + 2^9$ of F_5 .

C. F. Gauss¹³ proved that a regular polygon of m sides can be constructed by ruler and compasses if m is a product of a power of 2 and distinct odd primes each of the form F_n , and stated that the construction is impossible if m is not such a product. This subject will be treated under Roots of Unity.

Sebastiano Canterzani¹⁴ treated twenty cases, each with subdivisions depending on the final digits of possible factors, to find the factor 641 of F_5 ,

¹Oeuvres, 2, 1894, p. 206, letter to Frenicle, Aug. (?) 1640; 2, 1894, p. 309, letter to Pascal, Aug. 29, 1654 (Fermat asked Pascal to undertake a proof of the proposition, Pascal, III, 232; IV, 1819, 384); proposed to Brouncker and Wallis, June 1658, Oeuvres, 2, p. 404 (French transl., 3, p. 316). Cf. C. Henry, Bull. Bibl. Storia Sc. Mat. e Fis., 12, 1879, 500-1, 716-7; on p. 717, 42...1 should end with 7, *ibid.*, 13, 1880, 470; A. Genocchi, Atti Ac. Sc. Torino, 15, 1879-80, 803.

²Oeuvres, 1, 1891, p. 131 (French transl., 3, 1896, p. 120).

³Oeuvres, 2, 433-4, letter to Carcavi, Aug., 1659.

⁴Oeuvres, 2, 208, 212, letters from Fermat to Frenicle and Mersenne, Oct. 18 and Dec. 25, 1640.

⁵Disq. Arith., Art. 365. Cf. Werke, 2, 151, 159. Same view by Klügel, Math. Wörterbuch, 2, 1805, 211; 3, 1808, 896.

⁶Nouv. Corresp. Math., 5, 1879, 88, 122.

⁷Jour. für Math., 87, 1879, 172.

⁸Novarum Physico-Mathematicarum, Paris, 1647, 181.

⁹Corresp. Math. Phys. (ed., Fuss), I, 1843, p. 10, letter of Dec. 1729; p. 20, May 22, 1730; p. 32, July 1730.

¹⁰Comm. Ac. Petrop., 6, ad annos 1732-3 (1739), 103-7; Comm. Arith. Coll., 1, p. 2.

¹¹Novi Comm. Petrop., 1, 1747-8, p. 20 [9, 1762, p. 99]; Comm. Arith. Coll., 1, p. 55 [p. 357].

^{11a}Opera postuma, I, 1862, 169-171 (about 1770).

¹²Nouv. Mém. Ac. Berlin, année 1777, 1779, 239.

¹³Disq. Arith., 1801, Arts. 335-366; German transl. by Maser, 1889, pp. 397-448, 630-652.

¹⁴Mem. Ist. Naz. Italiano, Bologna, Mat., 2, II, 1810, 459-469.

and proved in the same lengthy dull manner that the quotient is a prime.

An anonymous writer¹⁵ stated that

$$(1) \quad 2+1, \quad 2^2+1, \quad 2^{2^2}+1, \quad 2^{2^{2^2}}+1, \dots$$

are all primes and are the only primes 2^k+1 . See Malvy.³⁹

Joubin¹⁶ suggested that these numbers (1) are possibly the ones really meant by Fermat,¹ evidently without having consulted all of Fermat's statements.

G. Eisenstein¹⁷ set the problem to prove that there is an infinitude of primes F_n .

E. Lucas¹⁸ stated that one could test the primality of F_6 in 30 hours by means of the series 3, 17, 577, . . . , each term being one less than the double of the square of the preceding. Then F_n is a prime if 2^{n-1} is the rank of the first term divisible by F_n , composite if no term is divisible by F_n . Finally, if a is the rank of the first term divisible by F_n , the prime divisors of F_n are of the form 2^kq+1 , where $k=a+1$ [not $k=2^{a+1}$]. See Lucas.²²

T. Pepin¹⁹ stated that the method of Lucas¹⁸ is not decisive when F_n divides a term of rank $a < 2^{n-1}$; for, if it does, we can conclude only that the prime divisors of F_n are of the form $2^{a+2}q+1$, so that we can not say whether or not F_n is prime if $a+2 \leq 2^{n-2}$. We may answer the question unambiguously by use of the new theorem: For $n > 1$, F_n is a prime if and only if it divides

$$k^{(F_n-1)/2}+1,$$

where k is any quadratic non-residue of F_n , as 5 or 10. To apply this test, take the minimum residues modulo F_n of

$$k^2, \quad k^4, \quad k^8, \dots, \quad k^{2^{n-1}}.$$

Proof was indicated by Lucas²⁹ of Ch. XVII, and by Morehead.⁵⁸

J. Pervouchine²⁰ (or Pervusin) announced, November 1877, that

$$F_{12} \equiv 0 \pmod{114689 = 7 \cdot 2^{14} + 1}.$$

E. Lucas²¹ announced the same result two months later and proved that every prime factor of F_n is $\equiv 1 \pmod{2^{n+2}}$.

Lucas²² employed the series 6, 34, 1154, . . . , each term of which is 2 less than the square of the preceding. Then F_n is a prime if the rank of the first term divisible by F_n is between 2^{n-1} and 2^n-1 , but composite if no term is divisible by F_n . Finally, if a is the rank of the first term divisible by F_n

¹⁵Annales de Math. (ed. Gergonne), 19, 1828-9, 256.

¹⁶Mémoire sur les facteurs numériques, Havre, 1831, note at end.

¹⁷Jour. für Math., 27, 1844, 87, Prob. 6.

¹⁸Comptes Rendus Paris, 85, 1877, 136-9.

¹⁹Comptes Rendus, 85, 1877, 329-331. Reprinted, with Lucas¹⁸ and Landry,²⁹ Sphinx-Oedipe, 5, 1910, 33-42.

²⁰Bull. Ac. St. Pétersbourg, (3), 24, 1878, 559 (presented by V. Bouniakowsky). Mélanges math. ast. sc. St. Pétersbourg, 5, 1874-81, 505.

²¹Atti R. Accad. Sc. Torino, 13, 1877-8, 271 (Jan. 27, 1878). Cf. Nouv. Corresp. Math., 4, 1878, 284; 5, 1879, 88. See Lucas⁴⁰ of Ch. XVII.

²²Amer. Jour. Math., 1, 1878, 313.

and if $a < 2^{n-1}$, the prime divisors of F_n are of the form* $2^k q + 1$, where $k = a + 1$ [cf. Lucas¹⁸]. He noted (p. 238) that a necessary condition that F_n be a prime is that the residue modulo F_n of the term of rank $2^n - 1$ in this series is zero. He verified (p. 292) that F_5 has the factor 641 and again stated that 30 hours would suffice to test F_6 .

F. Proth²³ stated that, if $k = 2^n$, $2^k + 1$ is a prime if and only if it divides $m = 3^{2^{k-1}} + 1$. He²⁴ indicated a proof by use of the series of Lucas defined by $u_0 = 0$, $u_1 = 1$, . . . , $u_n = 3u_{n-1} + 1$ and the facts that u_{p-1} is divisible by the prime p , while $m = u_{2^k}/u_{2^{k-1}}$. Cf. Lucas.²⁶

E. Gelin²⁵ asked if the numbers (1) are all primes. Catalan²⁵ noted that the first four are.

E. Lucas²⁶ noted that Proth's²³ theorem is the case $k = 3$ of Pepin's.¹⁹

Pervouchine²⁷ announced, February 1878, that F_{23} has the prime factor

$$5 \cdot 2^{25} + 1 = 167772161.$$

W. Simerka²⁸ gave a simple verification of the last result and the fact (Pervouchine²⁰) that $7 \cdot 2^{14} + 1$ divides F_{12} .

F. Landry,²⁹ when of age 82 and after several months' labor, found that

$$F_6 = 274177 \cdot 67280421310721,$$

the first factor being a prime. He and Le Lasseur and Gérardin^{29a} each proved that the last factor is a prime (cf. Lucas³¹).

K. Broda³⁰ sought a prime factor p of $a^{32} + 1$ by considering

$$n = (a^{32} - 1)(a^{64} + 1)(a^{512} + a^{384} + a^{256} + a^{128} + 1).$$

Multiply by $u = (a^{32} + 1)/p$. Thus $nu = (a^{640} - 1)/p$. But $a^{640} \equiv 1 \pmod{641}$. Since each factor of n is prime to p , we take $a = 2$ and see that $2^{32} + 1$ is divisible by 641.

E. Lucas³¹ stated that he had verified that F_6 is composite by his²² test, before Landry found the factors.

P. Seelhoff³² gave the factor $5 \cdot 2^{39} + 1$ of F_{36} and commented on Beguelin.¹²

*Lucas wrote $k = 2^a + 1$ in error, as noted by R. D. Carmichael on the proof-sheets of this History.

²³Comptes Rendus Paris, 87, 1878, 374.

²⁴Nouv. Corresp. Math., 4, 1878, 210-1; 5, 1879, 31.

²⁵Ibid., 4, 1878, 160.

²⁶Ibid., 5, 1879, 137.

²⁷Bull. Ac. St. Pétersbourg, (3), 25, 1879, 63 (presented by V. Bouniakowsky); Mélanges math. astr. ac. St. Pétersbourg, 5, 1874-81, 519. Cf. Nouv. Corresp. Math., 4, 1878, 284-5; 5, 1879, 22.

²⁸Casopis, Prag, 8, 1879, 36, 187-8. F. J. Studnicka, *ibid.*, 11, 1881, 137.

²⁹Comptes Rendus Paris, 91, 1880, 138; Bull. Bibl. Storia Sc. Mat., 13, 1880, 470; Nouv. Corresp. Math., 6, 1880, 417; Les Mondes, (2), 52, 1880. Cf. Seelhoff, Archiv Math. Phys., (2), 2, 1885, 329; Lucas, Amer. Jour. Math. 1, 1878, 292; Récréat. Math., 2, 1883, 235; l'intermédiaire des math., 16, 1909, 200.

^{29a}Sphinx-Oedipe, 5, 1910, 37-42.

³⁰Archiv Math. Phys., 68, 1882, 97.

³¹Récréations Math., 2, 1883, 233-5. Lucas,³² 354-5.

³²Zeitschr. Math. Phys., 31, 1886, 172-4, 380. For F_6 , p. 329. French transl., Sphinx-Oedipe, 1912, 84-90.

J. Hermes³³ indicated a test for composite F_n by Fermat's theorem.

R. Lipschitz³⁴ separated all integers into classes, the primes of one class being Fermat numbers F_n , and placed in a new light the question of the infinitude of primes F_n .

E. Lucas³⁵ stated the result of Proth,²³ but with a misprint [Cipolla⁴⁶].

H. Scheffler³⁶ stated that Legendre believed that every F_n is a prime(!), and obtained artificially the factor 641 of F_5 . He noted (p. 167) that

$$F_n F_{n+1} \dots F_{a-1} = 1 + 2^{2^n} + 2^{2 \cdot 2^n} + 2^{3 \cdot 2^n} + \dots + 2^{2^a - 2^n}.$$

He repeated (pp. 173-8) the test by Pepin,¹⁹ with $k = 3$, and (p. 178) expressed his belief that the numbers (1) are all primes, but had no proof for F_{16} .

W. W. R. Ball³⁷ gave references and quoted known results.

T. M. Pervouchine³⁸ checked his verification that F_{12} and F_{23} are composite by comparing the residues on division by $10^3 - 2$.

Malvy³⁹ noted that the prime $2^8 + 1$ is not in the series (1).

F. Klein⁴⁰ stated that F_7 is composite.

A. Hurwitz⁴¹ gave a generalization of Proth's²³ theorem. Let $F_n(x)$ denote an irreducible factor of degree $\phi(n)$ of $x^n - 1$. Then if there exists an integer q such that $F_{p-1}(q)$ is divisible by p , p is a prime. When $p = 2^k + 1$, $F_{p-1}(x) = x^{2^{k-1}} + 1$.

J. Hadamard⁴² gave a very simple proof of the second remark by Lucas.²¹

A. Cunningham⁴³ found that F_{11} has the factor 319489·974849.

A. E. Western⁴⁴ found that F_9 has the factor $2^{16} \cdot 37 + 1$, F_{18} the factor $2^{20} \cdot 13 + 1$, the quotient of F_{12} by the known factor $2^{14} \cdot 7 + 1$ has the factors $2^{16} \cdot 397 + 1$ and $2^{16} \cdot 7 \cdot 139 + 1$. He verified the primality of the factor $2^{41} \cdot 3 + 1$ of F_{38} , found by J. Cullen and A. Cunningham. He and A. Cunningham found that no more F_n have factors $< 10^6$ and similar results.

M. Cipolla⁴⁵ noted that, if q is a prime $> (9^{2^{m-2}} - 1)/2^{m+1}$ and $m > 1$, $2^m q + 1$ is a prime if and only if it divides $3^k + 1$ for $k = q \cdot 2^{m+1}$. He⁴⁶ pointed out the misprint in Lucas's³⁵ statement.

Nazarevsky⁴⁷ proved Proth's²³ result by using the fact that 3 is a primitive root of a prime $2^k + 1$.

³³Archiv Math. Phys., (2), 4, 1886, 214-5, footnote.

³⁴Jour. für Math., 105, 1889, 152-6; 106, 1890, 27-29.

³⁵Théorie des nombres, 1891, preface, xii.

³⁶Beiträge zur Zahlentheorie, 1891, 147, 151-2, 155 (bottom), 168.

³⁷Math. Recreations and Problems, ed. 2, 1892, 26; ed. 4, 1905, 36-7; ed. 5, 1911, 39-40.

³⁸Math. Papers Chicago Congress of 1893, I, 1896, 277.

³⁹L'intermédiaire des math., 2, 1895, 41 (219).

⁴⁰Vorträge über ausgewählte Fragen der Elementar Geometrie, 1895, 13; French transl., 1896, 26; English transl., "Famous Problems of Elementary Geometry," by Beman and Smith, 1897, 16.

⁴¹L'intermédiaire des math., 3, 1896, 214.

⁴²Ibid., p. 114.

⁴³Report British Assoc., 1899, 653-4. The misprint in the second factor has been corrected to agree with the true "value $2^{14} \cdot 7 \cdot 17 + 1$."

⁴⁴Cunningham and Western, Proc. Lond. Math. Soc., (2), 1, 1903, 175; Educ. Times, 1903, 270.

⁴⁵Periodico di Mat., 18, 1903, 331.

⁴⁶Also in Annali di Mat., (3), 9, 1904, 141.

⁴⁷L'intermédiaire des math., 11, 1904, 215.

A. Cunningham^{47a} noted that 3, 5, 6, 7, 10, 12 are primitive roots and 13, 15, 18, 21, 30 are quadratic residues of every prime $F_n > 5$. He factored $F_4^4 + 8 + (F_0 F_1 F_2 F_3)^4$.

Thorold Gosset⁴⁸ gave the two complex prime factors $a \pm bi$ of the known real factors of composite F_n , $n = 5, 6, 9, 11, 12, 18, 23, 36, 38$.

J. C. Morehead⁴⁹ verified by use of the criterion of Pepin¹⁹ with $k = 3$ that F_7 is composite, a result stated by Klein.⁴⁰

A. E. Western⁵⁰ verified in the same way that F_7 is composite. The work was done independently and found to agree with Morehead's.

J. C. Morehead⁵¹ found that F_{73} has the prime factor $2^{75} \cdot 5 + 1$.

A. Cunningham⁵² considered hyper-even numbers

$$E_{0,n} = 2^n, \quad E_{1,n} = 2^{E_{0,n}}, \dots, \quad E_{r+1,n} = 2^{E_{r,n}}.$$

For m odd, the residues modulo m of $E_{r,0}, E_{r,1}, \dots$ have a non-recurrent part and then a recurring cycle.

A. Cunningham⁵³ gave tables of residues of $E_{1,n}, E_{2,n}, E_{r,0}, 3^{3^n}$ and 5^{5^n} for the n 's forming the first cycle for each prime modulus < 100 and for certain larger primes. A hyper-exponential number is like a hyper-even number, but with base q in place of 2. He discussed the quadratic, quartic and octic residue character of a prime modulo F_n , and of F_n modulo F_{n+x} .

Cunningham and H. J. Woodall⁵⁴ gave material on possible factors of F_n .

A. Cunningham⁵⁵ noted that, for every $F_n > 5$, $2F_n = t^2 - (F_n - 2)u^2$ algebraically, and expressed F_5 and F_6 in two ways in each of the forms $a^2 + b^2$, $c^2 \pm 2d^2$. He⁵⁶ noted that $F_n^3 + E_n^3$ is the algebraic product of $n + 2$ factors, where $E_n = 2^{2^n}$, and that $M_n = (F_n^3 + E_n^3)/(F_n + E_n)$ is divisible by M_{n-r} . If $n - m \geq 2$, $F_m^4 + F_n^2$ is composite.

A. Cunningham⁵⁷ has considered the period of $1/N$ to base 2, where N is a product $F_m F_{m-1} \dots F_{m-r}$ of Fermat numbers.

J. C. Morehead and A. E. Western⁵⁸ verified by a very long computation that F_8 is composite. Use was made of the test by Pepin¹⁹ with $k = 3$, which was proved to follow from the converse of Fermat's theorem.

P. Bachmann⁵⁹ proved the tests by Pepin¹⁹ and Lucas.²²

A. Cunningham⁶⁰ noted that every $F_n > 5$ can be represented by 4 quadratic forms of determinants $\pm G_n, \pm 2G_n$, where $G_n = F_0 F_1 \dots F_{n-1}$.

Bisman¹⁴⁸ (of Ch. XIV) separated 16 cases in finding the factor 641 of F_5 .

^{47a}Math. Quest. Educ. Times, (2), 1, 1902, 108; 5, 1904, 71-2; 7, 1905, 72.

⁴⁸Mess. Math., 34, 1905, 153-4.

⁴⁹Bull. Amer. Math. Soc., 11, 1905, 543.

⁵⁰Proc. Lond. Math. Soc., (2), 3, 1905, xxi.

⁵¹Bull. Amer. Math. Soc., 12, 1906, 449; Annals of Math., (2), 10, 1908-9, 99. French transl. in Sphinx-Oedipe, Nancy, 1911, 49.

⁵²Report British Assoc. Adv. Sc., 1906, 485-6.

⁵³Proc. London Math. Soc., (2), 5, 1907, 237-274.

⁵⁴Messenger of Math., 37, 1907-8, 65-83.

⁵⁵Math. Quest. Educat. Times, (2), 12, 1907, 21-22, 28-31.

⁵⁶Ibid., (2), 14, 1908, 28; (2), 8, 1905, 35-6.

⁵⁷Math. Gazette, 4, 1908, 263.

⁵⁸Bull. Amer. Math. Soc., 16, 1909, 1-6. French transl., Sphinx-Oedipe, 1911, 50-55.

⁵⁹Niedere Zahlentheorie, II, 1910, 93-95.

⁶⁰Math. Quest. Educat. Times, (2), 20, 1911, 75, 97-98.

A. Gérardin⁶¹ noted that $F_n = (240x + 97)(240y + 161)$ for all the F_n fully factored to date, and specified x and y more exactly in special cases.

C. Henry⁶² gave references and quoted known results.

R. D. Carmichael⁶³ gave a test for the primality of F_n equivalent to Pepin's¹⁹ and a further generalization (p. 65) in the direction of Hurwitz's.⁴¹

R. C. Archibald⁶⁴ cited many of the papers listed above and collected in a table the known factors of F_n with the exception of that given by Morehead.⁵¹

For a remark on F_n , see Cunningham¹⁰¹ of Ch. VII.

⁶¹Sphinx-Oedipe, 7, 1912, 13.

⁶²Oeuvres de Fermat, 4, 1912, 202-4.

⁶³Annals of Math., (2), 15, 1913-4, 67.

⁶⁴Amer. Math. Monthly, 21, 1914, 247-251.

CHAPTER XVI.

FACTORS OF $a^n \pm b^n$.

Fermat¹ stated that $(2^p+1)/3$ has no factors other than $2kp+1$ if p is an odd prime.

L. Euler² noted that a^4+4b^4 has the factors $a^2 \pm 2ab + 2b^2$.

Euler³ discussed the numbers a for which a^2+1 is divisible by a prime $4n+1=r^2+s^2$. Let p/q be the convergent preceding r/s in the continued fraction for r/s ; then $ps-qr = \pm 1$. Thus every a is of the form $(4n+1)m \pm k$, where $k = pr+qs$.

Euler⁴ gave the 161 integers $a < 1500$ for which a^2+1 is a prime, and the cases $a = 1, 2, 4, 6, 16, 20, 24, 34$ for which a^4+1 is a prime.

Euler⁵ proved that, if m is a prime and a, b are relatively prime, a factor of $a^m - b^m$, not a divisor of $a - b$, is of the form $kn+1$. If $p = kn+1$ is a prime and $a = f^n \pm pa$, then $a^k - 1$ is divisible by p . If $af^m - bg^n$ is divisible by a prime $p = mn+1$, while f and g are not both divisible by p , then $a^m - b^m$ is divisible by p ; the converse is true if m and n are relatively prime.

Euler⁶ proved the related theorems: For q an odd prime, any prime divisor of $a^q - 1$, not a divisor of $a - 1$, is of the form $2nq+1$. If $a^m - 1$ is divisible by the prime $p = mn+1$, we can find integers x, y not divisible by p such that $A = ax^n - y^n$ is divisible by p (since the quotient of $a^m x^{mn} - y^{mn}$ by A is not divisible by p if x, y are suitably chosen).

Euler⁷ treated the problem to find all integers a for which a^2+1 is divisible by a given prime $4n+1 = p^2+q^2$. If a^2+b^2 is divisible by p^2+q^2 , there exist integers r, s such that $a = pr+qs, b = ps-qr$. We wish $b \neq \pm 1$. Hence we take the convergent r/s preceding p/q in the continued fraction for p/q . Thus $ps-qr = \pm 1$, and our answer is $a = \pm (pr+qs)$. He listed all primes $P = 4n+1 < 2000$ expressed as p^2+q^2 , and listed all the a 's for which a^2+1 is divisible by P . The table may be used to find all the divisors $< a$ of a given number a^2+1 . He gave his⁴ table and tabulated the values $a < 1500$ for which $(a^2+1)/k$ is a prime, for $k = 2, 5, 10$. He tabulated all the divisors of a^2+1 for $a \leq 1500$.

N. Beguelin⁸ stated that 2^n+1 has a trinary divisor $1+2^p+2^q$ only when $n = 10, 24, 32$, although his examples (p. 249) contradict this statement.

Euler⁹ gave a factor of $2^n \pm 1$ for various composite n 's.

¹Oeuvres, 2, 205, letter to Frenicle, Aug. (?), 1640. Bull. Bibl. St. Sc. Mat. e Fis., 12, 1879, 716.

²Corresp. Math. Phys. (ed., Fuss), I, 1843, p. 145; letter to Goldbach, 1742.

³Ibid., 242-3; letter to Goldbach, July 9, 1743.

⁴Ibid., 588-9, Oct. 28, 1752. Published, Euler.⁷

⁵Novi Comm. Petrop., 1, 1747-8, 20; Comm. Arith. Coll., 1, 57-61, and posthumous paper, *ibid.*, 2, 530-5; Opera postuma, I, 1862, 33-35. Cf. Euler¹⁵² of Ch. VII and the topic Quadratic Residues in Vol. III.

⁶Novi Comm. Petrop., 7, 1758-9 (1755), 49; Comm. Arith., 1, 269.

⁷Novi Comm. Petrop., 9, 1762-3, 99; Comm. Arith., 1, 358-369. French transl., Sphinx-Oedipe, 8, 1913, 1-12, 21-26, 64.

⁸Mém. Ac. Berlin, année 1777, 1779, 255. Cf. Ch. XV and Henry.¹⁴

⁹Posthumous paper, Comm. Arith., 2, 551; Opera postuma, I, 1862, 51.

Euler^{9a} discussed the divisors of numbers of the form $fa^4 + gb^4$.

Anton Felkel¹⁰ gave a table, incomplete as to a few entries, of the factors of $a^n - 1$, $n = 1, \dots, 11$; $a = 2, 3, \dots, 12$.

A. M. Legendre¹¹ proved that every prime divisor of $a^n + 1$ is either of the form $2nx + 1$ or divides $a^\omega + 1$ where ω is the quotient of n by an odd factor; every prime divisor of $a^n - 1$ is either of the form $nx + 1$ or divides $a^\omega - 1$ where ω is a factor of n . For n odd, the divisors must occur in $a(a^n \pm 1) = y^2 \pm a$ and are thus further limited by his tables III–XI of the linear forms of the divisors of $t^2 \pm au^2$.

C. F. Gauss¹² obtained by use of the quadratic reciprocity law the linear forms of the divisors of $x^2 - A$.

Gauss¹³ gave a table of 2452 numbers of the forms $a^2 + 1$, $a^2 + 4$, \dots , $a^2 + 81$ and their odd prime factors p , for certain a 's for which the p 's are all < 200 .

Sophie Germain¹⁴ noted that $p^4 + 4q^4$ has the factors $p^2 \pm 2pq + 2q^2$ [Euler²]. Taking $p = 1$, $q = 2^i$, we see that $2^{4i+2} + 1$ has the two factors $2^{2i+1} \pm 2^{i+1} + 1$.

F. Minding¹⁵ gave a detailed discussion of the linear forms of the divisors of $x^2 - c$, using the reciprocity law for the case of primes. He reproduced (pp. 188–190) the discussion by Legendre.¹¹

P. L. Tchebychef¹⁶ noted that, if p is an odd prime, every odd prime factor of $a^p - 1$ is either of the form $2pz + 1$ or is a factor of $a - 1$, and moreover is a divisor of $x^2 - ay^2$. Hence, for $a = 2$, it is of the form $2pz + 1$ and also of one of the forms $8m \pm 1$. Every odd prime factor of $a^{2n+1} + 1$ is either of the form $2(2n+1)z + 1$ or a divisor of $a + 1$ [cf. Legendre¹¹].

V. A. Lebesgue¹⁷ noted that the discussion of the linear forms of the divisors of $z^2 - D$, where D is composite, is simplified by use of Jacobi's generalization (a/b) of Legendre's symbol.

C. G. Reuschle¹⁸ denoted $(x^{ab} - 1)/(x^a - 1)$ by $F_a(b)$. Set $a = ab + b_1$, $b = a_1b_1 + b_2$, $b_1 = a_2b_2 + b_3, \dots$. If a, b are relatively prime,

$$\begin{aligned} \frac{1 - x^{ab}}{(x^a - 1)(x^b - 1)} &= \sum_{A=0}^{b-2} x^{Aa} F_b \{a(b-1-A)\} + x^b \sum_{A=0}^{b_1-2} x^{Ab} F_{b_1} \{a_1(b_1-1-A)\} \\ &+ \dots + x^{b+\beta_1+\dots+\beta_{n-2}} \sum_{A=0}^{b_{n-1}-2} x^{Ab_{n-2}} F_{b_{n-1}} \{a_{n-1}(b_{n-1}-1-A)\} + x^{b+\dots+\beta_{n-1}}. \end{aligned}$$

^{9a}Opera postuma, I, 1862, 161–7 (about 1773).

¹⁰Abhandl. d. Böhmischen Gesell. Wiss., Prag, 1, 1785, 165–170.

¹¹Théorie des nombres, 1798, pp. 207–213, 313–5; ed. 2, 1808, pp. 191–7, 286–8. German transl. by Maser, p. 222.

¹²Disq. Arith., 1801, Arts. 147–150.

¹³Werke, 2, 1863, 477–495. Schering, pp. 499–502, described the table and its formation by the composition of binary forms, e. g., $(a^2 + 1)\{(a+1)^2 + 1\} = \{a(a+1) + 1\}^2 + 1$.

¹⁴Manuscript 9118 fonds français Bibl. Nat. Paris, p. 84. Cf. C. Henry, Assoc. franç. avanc. sc., 1880, 205; Oeuvres de Fermat, 4, 1912, 208.

¹⁵Anfangsgründe der Höheren Arith., 1832, 59–70.

¹⁶Theorie der Congruenzen, in Russian, 1849; in German, 1889; §49.

¹⁷Jour. de Math., 15, 1850, 222–7.

¹⁸Math. Abhandlung, Stuttgart, 1853, II, pp. 6–13.

Reuschle's¹⁹ table A gives many factors of $a^3 \pm 1$, $a^4 \pm 1$, $a^5 \pm 1$, $a^{12} - 1$ for $a \leq 100$, and of $a^n - 1$ for $n \leq 42$, $a = 2, 3, 5, 6, 7, 10$.

Lebesgue^{19a} proved that $x^{p-1} + \dots + x + 1$ has no prime divisor other than the prime p and numbers of the form $kp + 1$.

Jean Plana²⁰ gave $3^{29} + 1 = 4.6091q$, $3^{29} - 1 = 2.59r$, and stated that q is a prime and that r has no factor < 52259 . But Lucas²⁵ noted that

$$q = 523 \cdot 5385997, \quad r = 28537 \cdot 20381027.$$

E. Kummer²¹ proved that there is no prime factor, other than t and numbers $2mt \pm 1$, of the cyclotomic function

$$x^e + x^{e-1} - (e-1)x^{e-2} - (e-2)x^{e-3} + \frac{1}{2}(e-2)(e-3)x^{e-4} + \dots$$

obtained from $(a^t - 1)/(a - 1)$ by setting $a + a^{-1} = x$, t being a prime $2e + 1$.

E. Catalan²² stated that, if $n = a + 1$ is odd, $a^n \mp 1$ is divisible by n^2 , but not by n^3 . Proof by Soons, *Mathesis*, (3), 2, 1902, 109.

H. LeLasseur and A. Aurifeuille²³ noted that $2^{4n+2} + 1$ has the factors $2^{2n+1} \pm 2^{n+1} + 1$ [cf. Euler,² S. Germain¹⁴].

E. Lucas²⁴ proved that $(2^{40} + 1)/(2^8 + 1)$ is a prime and gave the factors of $30^{15} \pm 1$, $2^{41} + 1$.

Theorems by Lucas on the factors of $a^n \pm b^n$, given in various papers in 1876-8, are cited in Ch. XVII.

Lucas²⁵ factored $(2m)^m \pm 1$ for $m = 7, 10, 11, 12, 14, 15$, and corrected Plana.²⁰

Lucas²⁶ gave tables due to LeLasseur and Aurifeuille of functions

$$\frac{x^n \pm y^n}{x \pm y} \quad (n \text{ odd}), \quad \frac{x^{2m} + y^{2m}}{x^2 + y^2},$$

expressed in the form $Y^2 \pm pxyZ^2$, which is factorable if $xy = pv^2$. Factors of $x^{10} + y^{10}$ are given for various x 's, y 's. He gave LeLasseur's table of the proper divisors of $2^n - 1$ for all odd values of $n < 100$ except $n = 61, 67, 71, 77, 79, 83, 85, 89, 93, 97$; the proper divisors of $2^n + 1$ for n odd and < 71 (except $n = 61, 67$) and for $n = 73, 75, 81, 83, 99, 135$; the proper divisors of $2^{2k} + 1$ for $2k \leq 74$ (except 64, 68) and for $2k = 78, 82, 84, 86, 90, 94, 102, 126$, etc. Lucas proved (pp. 790-4) that the proper divisors of $2^{4n} + 1$ are of the form $16nq + 1$, those of $a^{2abn} + b^{2abn}$ are of the form $8abnq + 1$; for n odd, those of $a^{abn} + b^{abn}$ are of the form $4abnq + 1$ if $ab = 4h + 1$, those of $a^{abn} - b^{abn}$ are of the form $4abnq + 1$ if $ab = 4h + 3$.

¹⁹Math. Abhandlung . . . Tabellen, Stuttgart, 1856. Full title in Ch. I.

^{19a}Comptes Rendus Paris, 51, 1860, 11.

²⁰Mem. Accad. Sc. Torino, (2), 20, 1863, 139-141.

²¹Cf. Bachmann, Kreistheilung, Leipzig, 1872.

²²Revue de l'Instruct. publique en Belgique, 17, 1870, 137; Mélanges Math., ed. 1, p. 40.

²³Atti R. Ac. Sc. Torino, 8, 1871; 13, 1877-8, 279. Nouv. Corresp. Math., 4, 1878, 86, 98.

Cf. Lucas,²⁵ p. 238; Lucas,²⁶ 784.

²⁴Nouv. Ann. Math., (2), 14, 1875, 523-5.

²⁵Amer. Jour. Math., 1, 1878, 293.

²⁶Bull. Bibl. Storia Sc. Mat. e Fis., 11, 1878, 783-798.

Lucas²⁷ gave the factors of $2^m + 1$ for $m = 4n \leq 60$ and for 72, 84; also for $m = 4n + 2 \leq 102$ and for 110, 114, 126, 130, 138, 150, 210.

E. Catalan²⁸ noted that $x^4 + 2(q-r)x^2 + q^2$ for $x^2 = (2r)^{2k+1}$ has the rational factors $(2r)^{2k+1} \pm (2r)^{k+1} + q$. The case $r = q = 1$ gives LeLasseur's²³ formula. Again, $3^{6k+3} + 1$ has the factors $3^{2k+1} + 1$, $3^{2k+1} \pm 3^{k+1} + 1$.

S. Réalis^{28a} deduced LeLasseur's²³ formula and $2^{4n} + 2^{2n} + 1 = \Pi(2^{2n} \pm 2^n + 1)$.

J. J. Sylvester²⁹ considered the cyclotomic function $\psi_i(x)$ obtained by setting $a + a^{-1} = x$ in the quotient by $a^{p^{(t)}/2}$ of

$$(1) \quad F_i(a) = \frac{(a^t - 1)\Pi(a^{t/p_1 p_2} - 1) \dots}{\Pi(a^{t/p_1} - 1) \dots} \quad (t = p_1^{e_1} \dots p_n^{e_n}),$$

where p_1, \dots, p_n are distinct primes. He stated that every divisor of $\psi_i(x)$ is of the form $kt \pm 1$, with the exception that, if $t = p^j (p \neq 1)/m$, p is a divisor (but not p^2). Conversely, every product of powers of primes of the form $kt \pm 1$ is a divisor of $\psi_i(x)$. Proofs were given by T. Pepin, *ibid.*, 526; E. Lucas, p. 855; Dedekind, p. 1205 (by use of ideals). Lucas added that $p = 2^{4h+3} - 1$ and $p = 2^{12h+5} - 1$ are primes if and only if they divide $\psi_{p+1}(x)$ for $x = \sqrt{-1}$ and $x = 3\sqrt{-1}$, respectively.

A. Lefébure³⁰ determined polynomials having no prime factor other than those of the form $HT + 1$, where H is given. First, let $T = n^t$, where n is a prime. For A, B relatively prime integers,

$$F_n(A, B) = \frac{A^n - B^n}{A - B}$$

has, besides n , no prime factor except those of the form $Hn^t + 1$, when A and B are exact n^{t-1} th powers of integers. Second, let $T = n^t m^h$, where n, m are distinct primes. The integral quotient of $F_n(u^m, v^m)$ by $F_n(u, v)$ has only prime factors of the form $Hn^t m^h + 1$ if u, v are powers of relatively prime integers with the exponent $m^{h-1} n^{t-1}$. Similarly, if T is a product of powers of several primes.

Lefébure³¹ discussed the decomposition into primes of $U^R - V^R$, where U, V are powers whose exponents involve factors of R .

E. Lucas³² stated that if n and $2n + 1$ are primes, then $2n + 1$ is a factor of $2^n - 1$ or $2^n + 1$ according as $n \equiv 3$ or $n \equiv 1 \pmod{4}$. If n and $4n + 1$ are primes, $4n + 1$ is a factor of $2^{2n} + 1$. If n and $8n + 1 = A^2 + 16B^2$ are primes, then $8n + 1$ is a factor of $2^{2n} + 1$ if B is odd, of $2^{2n} - 1$ if B is even. Also ten theorems stating when $6n + 1 = 4L^2 + 3M^2$, $12n + 1 = L^2 + 12M^2$ or $24n + 1 = L^2 + 48M^2$ are prime factors of $2^{kn} \pm 1$ for certain k 's.

²⁷Sur la série récurrente de Fermat, Rome, 1879, 9-10. Report by Cunningham.⁶³

²⁸Assoc. franç. avanc. sc., 9, 1880, 228.

^{28a}Nouv. Ann. Math., (2), 18, 1879, 500-9.

²⁹Comptes Rendus Paris, 90, 1880, 287, 345; Coll. Math. Papers, 3, 428. Incomplete in Math. Quest. Educ. Times, 40, 1884, 21.

³⁰Ann. sc. école norm. sup., (3), 1, 1884, 389-404; Comptes Rendus Paris, 98, 1884, 293, 413, 567, 613.

³¹Ann. sc. école norm. sup., (3), 2, 1885, 113.

³²Assoc. franç. avanc. sc., 15, 1886, II, 101-2.

A. S. Bang³³ discussed $F_t(a)$ defined by (1). If p is a prime, $F_p^k(a)$ has only prime factors $ap^k + 1$ if $d = a^{p^k-1} - 1$ is prime to p , but has the factor p (and not p^2) if d is divisible by p .

Bang³⁴ proved that, if $a > 1$, $t > 2$, $F_t(a)$ has a prime factor $at + 1$ except for $F_6(2)$.

L. Gianni³⁵ noted that if p is an odd prime dividing $a - 1$ and p^r divides $a^p - 1$, then p^{r-1} divides $a - 1$.

L. Kronecker³⁶ noted that, if $F_n(z)$ is the function whose roots are the $\phi(n)$ primitive n th roots of unity,

$$(x-y)^{\phi(n)} F_n\left(\frac{x+y}{x-y}\right) = G_n(x, y^2)$$

is an integral function involving only even powers of y . He investigated the prime factors q of $G_n(x, s)$ for s given. If q is prime to n and s , then q is congruent modulo n to Jacobi's symbol (s/q) . The same result was stated by Bauer.³⁷

J. J. Sylvester³⁸ called $\theta^m - 1$ the m th Fermatian function of θ .

Sylvester³⁹ stated that, for θ an integer $\neq 1$ or -1 ,

$$\theta_m \equiv \frac{\theta^m - 1}{\theta - 1}$$

contains at least as many distinct prime divisors as m contains divisors > 1 , except when $\theta = -2$, m even, and $\theta = 2$, m a multiple of 6, in which two cases the number of prime divisors may be one less than in the general case.

Sylvester⁴⁰ called the above θ_m a reduced Fermatian of index m . If $m = np^a$, n not divisible by the odd prime p , θ_m is divisible by p^a , but not by p^{a+1} , if $\theta - 1$ is divisible by p . If m is odd and $\theta - 1$ is divisible by each prime factor of m , then θ_m is divisible by m and the quotient is prime to m .

Sylvester^{40a} stated that if $P = 1 + p + \dots + p^{r-1}$ is divisible by q , and p, r are primes, either r divides $q - 1$ or $r = q$ divides $p - 1$. If $P = q^j$ and p, r, j are primes, j is a divisor of $q - r$. R. W. Genese easily proved the first statement and W. S. Foster the second.

T. Pepin⁴¹ factored various $a^n - 1$, including $a = 79, 67, 43$, $n = 5$; $a = 7$, $n = 11$; $a = 3$, $n = 23$; $a = 5$ or 7 , $n = 13$ (certain ones not in the tables by Bickmore⁴⁹).

H. Scheffler⁴² discussed the factorization of $2^r + 1$ by writing possible factors to the base 2, as had Beguelin.⁸ He noted (p. 151) that, if $m = 2^{n-1}$,

$$1 + 2^{(2m+1)n} = (1 + 2^n)^2 \{ 1 - 2m + (2m-1)2^n - (2m-2)2^{2n} \\ + \dots - 2 \cdot 2^{(2m-2)n} + 2^{(2m-1)n} \}.$$

His formula (top p. 156), in which 2^{n-1} is a misprint for 2^{2n-1} , is equivalent to that of LeLasseur.²³

³³Tidsskrift for Mat., (5), 4, 1886, 70-80. ³⁴Ibid., 130-137. ³⁵Periodico di Mat., 2, 1887, 114.

³⁶Berlin Berichte, 1888, 417; Werke, 3, I, 281-292. ³⁷Jour. für Math., 131, 1906, 265-7.

³⁸Nature, 37, 1888, 152. ³⁹Ibid., p. 418; Coll. Papers, 4, 1912, 628.

⁴⁰Comptes Rendus Paris, 106, 1888, 446; Coll. Papers, 4, 607.

^{40a}Math. Quest. Educ. Times, 49, 1888, 54, 69.

⁴¹Atti Accad. Pont. Nuovi Lincei, 49, 1890, 163. Cf. Escott, Messenger Math., 33, 1903-4, 49.

⁴²Beiträge zur Zahlentheorie, 1891, 147-178.

E. Lucas⁴³ gave algebraic factors of

$$x^6 + 27y^6, \quad x^{10} - 5^5y^{10}, \quad x^{12} + 6^6y^{12}.$$

K. Zsigmondy⁴⁴ proved the existence of a prime dividing $a^\gamma - b^\gamma$, but no similar binomial with a lower exponent, exceptions apart (cf. Bang,^{33, 34} Birkhoff⁶²).

J. W. L. Glaisher⁴⁵ gave the prime factors of $p^6 - (-1)^{(p-1)/2}$ for each prime $p < 100$.

T. Pepin⁴⁶ proved that $(31^7 - 1)/30$, $(83^5 - 1)/82$, $(2^{41} + 1)/(3 \cdot 83)$ are primes.

A. A. Markoff⁴⁷ investigated the greatest prime factor of $n^2 + 1$.

W. P. Workman⁴⁸ noted the factors of $3^{6k+3} + 1$ [due to Catalan²⁸] and $2^{54} + 1$, and stated that Lucas⁴³ (p. 326) gave erroneous factors of $2^{58} + 1$.

C. E. Bickmore⁴⁹ gave factors of $a^n - 1$ for $n \leq 50$, $a = 2, 3, 5, 6, 7, 10, 11, 12$.

Several^{49a} proved that $n^n - 1$ is divisible by $4n + 1$ if $4n + 1$ is prime.

A. Cunningham⁵⁰ gave 43 primes exceeding 9 million which are factors of $(x^5 \pm 1)/(x \pm 1)$, and factors of $3^{30} + 1$, $3^{33} - 1$, $3^{63} + 1$, $3^{105} + 1$, $5^{13} - 1$, $5^{14} + 1$, $5^{17} - 1$, $5^{20} + 1$, $5^{35} - 1$.

A. Cunningham⁵¹ considered at length the factorization of Aurifeuillians, i. e., the algebraically irreducible factors of

$$(n_1x^2)^{2n} + (2n_2y^2)^{2n}, \quad (n_1x^2)^n + (-1)^{\frac{n+1}{2}}(n_2y^2)^n \quad (n_1n_2 = n),$$

where n_1 and x are relatively prime to n_2 and y , while n has no square factor, and is odd in the second case. Aurifeuille had found them to be expressible algebraically in the form $P^2 - Q^2$. There are given factors of $2^n + 1$ for n even and ≤ 102 , and for $n = 110, 114, 126, 130, 138, 150, 210$.

A. Cunningham⁵² factored numbers $a^n \pm 1$ by use of tables, complete to $p = 101$, giving the lengths l of the periods of primes p and their powers < 10000 to various bases q , so that $q^l \equiv 1 \pmod{p}$ or p^k .

A. Cunningham and H. J. Woodall⁵³ gave factors of $N = 2^x 10^a \pm 1$ for $x \leq 30$, $a \leq 10$, and for further sets; also, for each prime $p \leq 3001$, the least a and the least corresponding x for which p is a divisor of N . Bickmore (p. 95) gave the linear and quadratic forms of factors of N .

T. Pepin⁵⁴ factored $a^7 - 1$ for $a = 37, 41, 79$; also⁵⁵ $151^5 - 1$.

⁴³Théorie des nombres, 1891, 132, exs. 2-4.

⁴⁴Monatshefte Math. Phys., 3, 1892, 283. Details in Ch. VII, Zsigmondy.⁷⁸

⁴⁵Quar. Jour. Math., 26, 1893, 47.

⁴⁶Memorie Accad. Pont. Nuovi Lincei, 9, I, 1893, 47-76.

⁴⁷Comptes Rendus Paris, 120, 1895, 1032. ⁴⁸Messenger Math., 24, 1895, 67.

⁴⁹*Ibid.*, 25, 1896, 1-44; 26, 1897, 1-38; French transl., Sphinx-Oedipe, 7, 1912, 129-44, 155-9.

^{49a}Math. Quest. Educ. Times, 65, 1896, 78; (2), 8, 1905, 97.

⁵⁰Proc. London Math. Soc., 28, 1897, 377, 379. ⁵¹*Ibid.*, 29, 1898, 381-438.

⁵²Messenger Math., 29, 1899-1900, 145-179. The line of $N^4 = 53^2$ (p. 17) is incorrect.

⁵³Math. Quest. Educat. Times, 73, 1900, 83-94. [Some errors.]

⁵⁴Mem. Pont. Ac. Nuovi Lincei, 17, 1900, 321-344; errata, 18, 1901. Cf. Sphinx-Oedipe, 5, 1910, numéro spécial, 1-9. Cf. Jahrbuch Fortschritte Math., on $a = 37$.

⁵⁵Atti Accad. Pont. Nuovi Lincei, 44, 1900-1, 89.

A. Cunningham⁵⁶ factored $5^n - 1$ for $n = 75, 105$.

L. Kronecker^{56a} proved that every divisor, prime to t , of (1) is $\equiv 1 \pmod{t}$.

H. S. Vandiver^{56b} noted that the proof applies to the homogeneous form $F_t(a, b)$ of (1) if a, b are relatively prime.

D. Biddle⁵⁷ gave a defective proof that $3 \cdot 2^{41} + 1$ is a prime.

The Math. Quest. Educational Times contains the factorizations of:

Vol. 66 (1897), p. 97, $2^{155} - 1$ factor 31^2 . Vol. 68 (1898), p. 27, p. 112, $2^{720} - 1$; p. 114, $10^{12} + 4$.

Vol. 69 (1898), p. 61, $382^4 + 1$; p. 73, $x^5 - 1$, $x = 500, 2000$; p. 117, $x^6 + y^6$; p. 118, $10^{18} + 3^3$, $3^3 \cdot 10^{18} + 1$.

Vol. 70 (1899), p. 32, p. 69, $242^{10} + 1$; p. 47, $320^{15} - 1$; p. 64, $2^{22} + 1$, $8^{14} + 1$, $200^{18} + 1$; p. 72, $20^{14} - 1$; p. 107, $972^{15} + 1$. Vol. 71 (1899), p. 63, $x^{4n+2} - 1$; p. 72, $x^4 + y^4$.

Vol. 72 (1900), p. 61, $(3n)^{4n} - 1$ factor $24n + 1$ if prime; p. 86, $722^{10} + 1$; p. 117, $1440^{10} + 1$.

Vol. 73 (1900), p. 51, $35^{20} + 1$; p. 96, $7^{11} - 1$; p. 104, p. 114, $x^4 + y^4$.

Vol. 74 (1901), p. 27, a prime $2^q q + 1$ divides $q^k - 1$ if $k = 2^{q-1}$; p. 86, $x^{10} - 5^5 y^{10}$.

Vol. 75 (1901), p. 37, $x^4 + y^4$; p. 90, $1792^7 + 1$; p. 111, $7^{35} + 1$. [Educ. Times, (2), 54, 1901, 223, 260].

Ser. 2, Vol. 1 (1902), p. 46, $10082^6 + 1$; p. 84, $x^4 + \mu y^4$. Vol. 2 (1902), p. 33, p. 53, $N^4 + 1$; p. 118, $11^{33} + 1$.

Vol. 3 (1903), p. 49, $a^4 + b^4$ (cf. 74, 1901, 44); p. 114, $a^6 + 1$, $a = 60000$.

Vol. 6 (1904), p. 62, $96^{18} + 1$.

Vol. 7 (1905), p. 62, $208^{13} - 1$; pp. 106-7, $2^{126} + 1$.

Vol. 8 (1905), p. 50, $96^{18} + 1$; p. 64, $2^{126} + 1$.

Vol. 10 (1906), p. 36, $54^{18} + 1$, $6^{54} + 1$.

Vol. 12 (1907), p. 54, $6^{42} + 1$, $24^{30} + 1$.

Vol. 13 (1908), p. 63, $106 - 7$, $3^{54} + 2^{54}$.

Vol. 14 (1908), p. 17, $150^{18} + 1$; p. 71, sextics; p. 96, $7^{35} + 1$.

Vol. 15 (1909), p. 57, $3^{54} + 2^{54}$; p. 33, $3^{111} + 1$, $12^{45} + 1$; p. 103, $28^{21} + 1$, $44^{11} + 1$, $6^{30} + 1$.

Vol. 16 (1909), p. 21, $19^{24} + 1$.

Vol. 18 (1910), pp. 53-5, $102 - 3$, $x^4 + 4y^4$; pp. 69-71, $x^6 + 27y^6$; p. 93, $y^{16} - 1$.

Vol. 19 (1911), p. 103, $x^3 + y^3 = z^3 + w^3$. Vol. 23 (1913), p. 92, $(x^2 - Nx + N)^4 + N(x^2 - N)^4$.

Vol. 24 (1913), pp. 61-2, $x^{2y} \pm y^y$, $y = 5, 7, 11, 13$; pp. 71-2, $x^{12} + 2^6$, $x^{18} + 3^9$, $x^{30} + 3^{15}$.

Vol. 26 (1914), p. 23, $x^{2k} + 1$ for $k = 6n + 3 \not\equiv 3^y$; p. 39, $x^{12} + 6^6$; p. 42, $x^{10} - 5^5$, $x^{14} + 7^7$, $x^{22} + 11^{11}$, $x^{26} - 13^{13}$. Vol. 27 (1915), pp. 65-6, $45^{15} - 1$, $20^{25} - 1$, $k^{30} + 1$ for $k = 6, 8, 10$; p. 83, $x^4 + 4y^4$ (when four factors). Vol. 28 (1915), p. 72, $50^{30} + 1$. Vol. 29 (1916), p. 95, $96^{18} + 1$.

New series, vol. 1 (1916), p. 86, $x^{20} + 10^{10}$, $x^{28} + 14^{14}$; pp. 94-5, $x^{30} - 5^{15}$, $x^{30} + 15^{15}$.

Vol. 2 (1916), p. 19, $x^{30} - 5^{15}$.

Vol. 3 (1917), p. 16, $x^{15} - y^{15}$; p. 52, $x^{11} - 1$.

E. B. Escott⁵⁸ gave many cases when $1 + x^2$ is a product of two powers of primes or the double of such a product.

⁵⁶Proc. London Math. Soc., 34, 1901, 49.

^{56a}Vorlesungen über Zahlentheorie, 1, 1901, 440-1.

^{56b}Amer. Math. Monthly, 10, 1903, 171.

⁵⁷Messenger Math., 31, 1901-2, 116 (error); 33, 1903-4, 126.

⁵⁸L'intermédiaire des math., 7, 1900, 170.

P. F. Teilhet⁵⁹ gave formulas factoring cases of $1+x^2$, as

$$(b^2+b+1)^2+1=[(b+1)^2+1](b^2+1),$$

$$4(c+1)^4+1=[(c+2)^2+(c+1)^2][(c+1)^2+c^2],$$

the last being (10, 1903, 170) a case of the known formula for the product of two sums of two squares (cf. 11, 1904, 50).

Escott⁶⁰ repeated Euler's⁷ remarks on the integers x for which $1+x^2$ is divisible by a given prime. He and Teilhet (11, 1904, 10, 203) noted that any common divisor of b and $a \neq 1$ divides $(a^b \pm 1)/(a \pm 1)$.

G. Wertheim⁶¹ collected the theorems on the divisors of $a^m \pm 1$.

G. D. Birkhoff and H. S. Vandiver⁶² employed relatively prime integers a, b ($a > b$) and defined a primitive divisor of $V_n = a^n - b^n$ to be one relatively prime to V_m , for all divisors m of n . They proved that, if $n \neq 2$, V_n has a primitive divisor $\neq 1$ except for $n=6$, $a=2$, $b=1$.

L. E. Dickson^{62a} noted that $(p^4-1)(p^2-1)$ has no factor $\equiv 1 \pmod{p^3}$ if p is prime.

A. Cunningham⁶³ gave high primes y^2+1 , $(y^2+1)/2$, y^2+y+1 .

H. J. Woodall⁶⁴ gave factors of y^2+1 .

J. W. L. Glaisher⁶⁵ factored $2^{2r} \pm 2^r + 1$ for $r \leq 11$, in connection with the question of the similarity of the n th pedal triangle to a given triangle.

L. E. Dickson⁶⁶ gave a new derivation of (1), found when $F_t(a)$ is divisible by p_1 or p_1^2 , where p_1 is a prime factor of t , and proved that, if a is an integer > 1 , $F_t(a)$ has a prime factor not dividing $a^m - 1$ ($m < t$) except in the cases $t=2$, $a=2^k-1$, and $t=6$, $a=2$; whence a^t-1 has a prime factor not dividing a^m-1 ($m < t$) except in those cases [cf. Birkhoff,⁶² Carmichael⁷⁵].

Dickson⁶⁷ applied the last theorem to the theory of finite algebras and gave material on the factors of p^n-1 .

A. Cunningham⁶⁸ treated at length the factorization of y^n+1 for $n=2, 4, 8, 16$, and $(y^{3n}+1)/(y^n+1)$ for $n=1, 2, 4, 8$, by means of extensive tables of solutions of the corresponding congruences modulo p . He discussed also x^n+y^n , $n=4, 6, 8, 12$.

Cunningham^{68a} factored $\lambda(x^5-y^5)/(x-y) + \mu(x^6+y^6)/(x^2+y^2)$ by expressing the fractions in the form $P^2 - kxyQ^2$, $k=5, 6$.

⁵⁹L'intermédiaire des math., 9, 1902, 316-8.

⁶⁰Ibid., 12, 1905, 38; cf. 11, 1904, 195-6.

⁶¹Anfangsgründe der Zahlenlehre, 1902, 297-303, 314.

⁶²Annals of Math., 5, 1903-4, 173. Cf. Zsigmondy,⁴⁴ Dickson.⁶⁶

^{62a}Amer. Math. Monthly, 11, 1904, 197, 238; 15, 1908, 90-1.

⁶³Quar. Jour. Math., 35, 1904, 10-21.

⁶⁴Ibid., p. 95.

⁶⁵Ibid., 36, 1905, 156.

⁶⁶Amer. Math. Monthly, 12, 1905, 86-89.

⁶⁷Göttingen Nachrichten, 1905, 17-23.

⁶⁸Messenger Math., 35, 1905-6, 166-185; 36, 1907, 145-174; 38, 1908-9, 81-104, 145-175; 39, 1909, 33-63, 97-128; 40, 1910-11, 1-36. Educat. Times, 60, 1907, 544; Math. Quest. Educat. Times, (2), 13, 1908, 95-98; (2), 14, 1908, 37-8, 52-3, 73-4; (2), 15, 1909, 33-4, 103-4; (2), 17, 1910, 88, 99. Proc. London Math. Soc., 27, 1896, 98-111; (2), 9, 1910, 1-14.

^{68a}Math. Quest. Educ. Times, 10, 1906, 58-9.

L. E. Dickson and E. B. Escott⁶⁹ discussed the divisibility of $p^{n/\delta} - 1$ by $d(p^{n/d} - 1)$, where d is a divisor of n , and δ of d .

R. D. Carmichael⁷⁰ proved that if $P^{\delta a} - R^{\delta a}$ is divisible by δa and we set $Q = (P^a - R^a)/\{a(P - R)\}$, then Q/δ is an integer if and only if a is divisible by the least integer e for which $P^e - R^e$ is divisible by each prime factor of a not dividing $P - R$, and δ is a divisor of Q . Proof for the case $R = 1$ had been given by E. B. Escott⁷¹.

A. Cunningham⁷² tabulated the factors of $y^{105} \pm 1$ for $y = 2, 3, 5, 7, 12$.

K. J. Sanjana⁷³ considered the factors of

$$(x^{(2n+1)k} \pm 1)/(x^k \pm 1).$$

Sanjana^{73a} applied his method to prove the statement of M. Kannan that $20^{45} - 1 = 11 \cdot 19 \cdot 31 \cdot 61 \cdot 251 \cdot 421 \cdot 3001 \cdot 261451 \cdot 64008001 \cdot 3994611390415801 \cdot 4199436993616201$.

L. E. Dickson⁷⁴ factored $n^n - 1$ for various values of n .

R. D. Carmichael⁷⁵ employed the methods of Dickson⁶⁶ to obtain generalizations. Let $Q_n(a, \beta)$ be the homogeneous form of $F_n(a)$. Let $n = \prod p_i^{a_i}$, where the p 's are distinct primes, and let c be a divisor of n and a multiple of $p_1^{a_1}$. If a, β are relatively prime, the g. c. d. of $\delta = a^{n/p_1} - \beta^{n/p_1}$ and $Q_c(a, \beta)$ is 1 or p_1 and at most one $Q_c(a, \beta)$ contains the factor p_1 when δ contains p_1^2 ; if $p_1 > 2$ divides δ , at most one $Q_c(a, \beta)$ contains p_1 , and no one of them contains p_1^2 . If a, β are relatively prime and $c = mp_1^{a_1}$, where $m > 1$ and m is prime to p_1 , then $Q_c(a, \beta)$ is divisible by p_1 if and only if $a^x \equiv \beta^x \pmod{p_1}$ holds for $x = m$, but not for $0 < x < m$; in all other cases $Q \equiv 1 \pmod{m}$. If a, β are relatively prime, $Q_c(a, \beta)$, and hence also $a^c - \beta^c$, has a prime factor not dividing $a^s - \beta^s$ ($s < c$), except in the cases (i) $c = 2$, $\beta = 1$, $a = 2^k - 1$; (ii) $Q_c(a, \beta) = p =$ greatest prime factor of c , and $a^{n/p} \equiv \beta^{n/p} \pmod{p}$; (iii) $Q_c(a, \beta) = 1$.

E. Miot⁷⁶ noted that LeLasseur's²³ formula is the case $m = n = 1$ of

$$\left(\frac{2^{2k+1}n^2}{m}\right)^2 + m^2 = \Pi \left(m + \frac{2^{2k+1}n^2}{m} \pm 2^{k+1}n\right).$$

Welsch (p. 213) stated that the latter is no more general than the case $k = 0$, which follows from the known formula for the product of two sums of two squares.

A. Cunningham⁷⁷ noted the decomposition into primes:

$$2^{77} + 1 = 3 \cdot 43 \cdot 617 \cdot 683 \cdot 78233 \cdot 35532364099.$$

⁶⁹L'intermédiaire des math., 1906, 87; 1908, 135; 18, 1911, 200. Cf. Dickson.⁶⁷

⁷⁰Amer. Math. Monthly, 14, 1907, 8-9.

⁷¹Ibid., 13, 1906, 155-6.

⁷²Report British Assoc., 78, 1908, 615-6.

⁷³Proc. Edinburgh Math. Soc., 26, 1908, 67-86; corrections, 28, 1909-10, viii.

^{73a}Jour. Indian Math. Club, 1, 1909, 212.

⁷⁴Messenger Math., 38, 1908, 14-32, and Dickson¹¹⁸⁻⁹ of Ch. XIV.

⁷⁵Amer. Math. Monthly, 16, 1909, 153-9.

⁷⁶L'intermédiaire des math., 17, 1910, 102.

⁷⁷Report British Assoc. for 1910, 529; Proc. London Math. Soc., (2), 8, 1910, xiii.

A. Cunningham⁷⁸ discussed quasi-Mersenne numbers $N_q = x^q - y^q$, with $x - y = 1$, q a prime, tabulating every prime factor < 1000 for $q < 50$, $x < 20$ if $q > 5$, $x < 50$ if $q = 5$, and treated Aurifeuillians

$$(X^q \pm Y^q)/(X \pm Y), \quad X = \xi^2, \quad Y = q\eta^2.$$

H. C. Pocklington⁷⁹ proved that, if n is prime, $(x^n - y^n)/(x - y)$ is divisible only by numbers of the form $mn + 1$ unless $x - y$ is divisible by n [Euler], and then is divisible only by n and numbers of the forms $mn + 1$, $n(mn + 1)$.

G. Fontené⁸⁰ stated that, if p is a prime and x, y are relatively prime, each prime factor of $(x^p - y^p)/(x - y)$ is of the form $kp + 1$, except for a factor p , occurring if $x \equiv y \pmod{p}$ and then only to the first power if $p > 2$.

G. Fontené⁸¹ considered the homogeneous form $f_n(x, y)$ derived from (1) by setting $a = x/y$. If p^a is the highest power of a prime p dividing n ,

$$f_n \equiv (f_{n/p^a})^{p^a} \pmod{p}, \quad x^n - y^n \equiv (x^{n/p^a} - y^{n/p^a})^{p^a} \pmod{p}.$$

The main theorem proved is the following: If x, y are relatively prime every prime divisor of $f_n(x, y)$ is of the form $kn + 1$, unless it is divisible by the greatest prime factor (say p) of n . It has this factor p if $p - 1$ is divisible by n/p^a and if x, y satisfy $f_{n/p^a} \equiv 0 \pmod{p}$, the latter having for each y prime to p a number of roots x equal to the degree of the congruence. In particular, if n is a power of a prime p , every prime factor of f_n is of the form $kn + 1$, with the exception of a divisor p occurring if $x \equiv y \pmod{p}$, and then to the first power if $n \neq 2$.

J. G. van der Corput⁸² considered the properties of the factors of the expression derived from $a^t + b^t$ as (1) is derived from $a^t - 1$.

A. Gérardin⁸³ factored $a^8 + b^8$ in four numerical cases and gave

$$(a^2 + 3\beta^2)^4 + (4a\beta)^4 = \Pi \{ (3a^2 \pm 2a\beta + 3\beta^2)^2 - 2(2a^2 \pm 2a\beta)^2 \}.$$

A. Cunningham⁸⁴ tabulated factors of $y^4 \pm 2$, $2y^4 \pm 1$.

R. D. Carmichael⁸⁵ treated at length the numerical factors of $a^n \pm \beta^n$ and the homogeneous form $Q_n(a, \beta)$ of (1), when $a + \beta$ and $a\beta$ are relatively prime integers, while a, β may be irrational.

A. Gérardin^{85a} factored $x^4 + 1$ for $x = 373, 404, 447, 508, 804, 929$; investigated $x^4 - 2$ for $x \leq 50$, $y^4 - 8$ for $y \leq 75$, $8v^4 - 1$ for $v \leq 25$, $2w^4 - 1$ for $w \leq 37$, and gave ten methods of factoring numbers $\lambda a^4 - 1$.

L. Valroff^{85b} factored $2x^4 - 1$ for $101 \leq x \leq 180$, $8x^4 - 1$ for $x < 128$.

A. Gérardin^{85c} expressed 622833161 (a factor of $20^{10} + 1$) as a sum of two squares in two ways to get its prime factors 2801 and 222361.

⁷⁸Messenger Math., 41, 1911-12, 119-145.

⁷⁹Proc. Cambr. Phil. Soc., 16, 1911, 8.

⁸⁰Nouv. Ann. Math., (4), 9, 1909, 384; proof, (4), 10, 1910, 475; 13, 1913, 383-4.

⁸¹Ibid., (4), 12, 1912, 241-260.

⁸²Nieuw Archief voor Wiskunde, (2), 10, 1913, 357-361.

⁸³Wiskundig Tijdschrift, 10, 1913, 59.

⁸⁴Messenger Math., 43, 1913-4, 34-57.

⁸⁵Annals of Math., (2), 15, 1913-4, 30-70.

^{85a}Sphinx-Oedipe, 1912, 188-9; 1913, 34-44; 1914, 20, 23-8, 34-7, 48.

^{85b}Ibid., 1914, 5-6, 18-9, 28-30, 33, 37, 73.

^{85c}Ibid., 39. Stated by E. Fauquembergue, l'intermédiaire des math., 21, 1914, 45.

A. Cunningham⁸⁶ tabulated factors of $y^y \pm 1$, $x^{xy} \pm y^{xy}$, and gave an account of printed and manuscript tables of solutions of $y^m \pm 1 \equiv 0 \pmod{p^k}$.

Cunningham⁸⁷ tabulated factors of $x^y \pm y^x$ for $x \leq 16$ and certain y 's as high as 31 when $x = 2$ or 4, where x, y are relatively prime and $x > 1$, $y > 1$.

Cunningham⁸⁸ noted that $x \cdot 2^x + 1$ is composite for $1 < x < 233$, $x \neq 141$.

A. Cunningham and H. J. Woodall⁸⁹ tabulated factors of $2^q \pm q$ and $q \cdot 2^q \pm 1$ for $q \leq 66$, and tabulated values of q for which one of these four functions is divisible by a given prime p or power of p . They confirmed that $x \cdot 2^x + 1$ is composite when $1 < x < 233$ except perhaps when $x = 141$. Incidentally (p. 15), the factors of $2^k \pm k - 1$ for $k \leq 17$ are given.

For factors of $2^n - 1$ and $10^n - 1$, see Chapters I and VI. For factor tables of numbers $m \cdot 2^k \pm 1$, see Seelhoff⁷² and Morehead⁹⁰ of Ch. XIII; for $m \cdot 6^k \pm 1$, Dines⁹¹. For factors of several numbers $a^n - 1$, see Lawrence¹⁵, Biddle¹⁶, and Kraitchik²¹ of Ch. XIV. For the form of factors of $a^k + b^k$ when $k = 2^n$, see Euler¹¹ of Ch. XV. Various results in Ch. XVII relate to factors of $a^n \pm b^n$.

FACTORS OF TRINOMIALS.

Seven⁹⁵ primes p such that $(p^2 - 1)^2$ has 4 or more factors $px + 1$, $x < p$. List⁹⁶ of algebraically factorable trinomials $x^5 + xy^4 + y^5$, etc.

Factors⁹⁷ of $14^8 + 14^5 + 1$, $7^8 + 2 \cdot 7^5 + 1$, etc.

Conditions that $x^8 + Px^4 + c^8$ be a product of 4 rational quadratic factors.⁹⁸

Two⁹⁹ factors of $x^8 + (4m^4 + 8m^2 + 2)x^4y^4 + y^8$.

Factors¹⁰⁰ of various trinomial expressions.

For factors of $x^4 + 6bx^2 + b^2$ see Dirichlet⁹ of Ch. XVII. See papers 28, 28a, 65, 89 above.

⁸⁶Messenger Math., 45, 1915, 49-75.

⁸⁷*Ibid.*, 185-192.

⁸⁸Proc. London Math. Soc., (2), 4, 1907, xviii; (2), 15, 1916-7, xxix.

⁸⁹Messenger Math., 47, 1917, 1-38. Math. Quest. Educ. Times, (2), 10, 1906, 44.

⁹⁰Math. Quest. Educat. Times, (2), 15, 1909, 82-3. Amer. Math. Monthly, 15, 1908, 67, 138.

L'intermédiaire des math., 15, 1908, 121.

⁹¹Math. Quest. Educ. Times, (2), 16, 1909, 39-41.

⁹²*Ibid.*, 65-6.

⁹³*Ibid.*, (2), 18, 1910, 64-5; (2), 22, 1912, 20-1.

⁹⁴Sphinx-Oedipe, 6, 1911, 8-9.

¹⁰⁰Math. Quest. Educ. Times, 72, 1900, 26-8; 74, 1901, 130-1; (2), 6, 1904, 97; 19, 1911, 85; 20, 1911, 25-6, 76-8; 22, 1912, 54-61. Math. Quest. and Solutions, 3, 1917, 66; 4, 1917, 13, 39; 5, 1918, 38, 50-1.

CHAPTER XVII.

RECURRING SERIES; LUCAS' u_n, v_n .

Leonardo Pisano¹, or Fibonacci, employed, in 1202 (revised manuscript, 1228), the recurring series 1, 2, 3, 5, 8, 13, . . . in a problem on the number of offspring of a pair of rabbits. We shall write U_n for the n th term, and u_n for the $(n+1)$ th term of 0, 1, 1, 2, 3, 5, . . . derived by prefixing 0, 1 to the former series.

Albert Girard² noted the law $u_{n+2} = u_{n+1} + u_n$ for these series.

Robert Simson³ noted that this series is given by the successive convergents to the continued fraction for $(\sqrt{5}+1)/2$. The square of any term is proved to differ from the product of the two adjacent terms by ± 1 .

L. Euler⁴ noted that $(a+\sqrt{b})^k = A_k + B_k\sqrt{b}$ implies

$$A_k = \frac{1}{2}\{(a+\sqrt{b})^k + (a-\sqrt{b})^k\}, \quad B_k = \frac{1}{2\sqrt{b}}\{(a+\sqrt{b})^k - (a-\sqrt{b})^k\}.$$

J. L. Lagrange⁵ noted that the residues of A_k and B_k with respect to any modulus are periodic.

Lagrange⁶ proved that if the prime p divides no number of the form $t^2 - au^2$, then p divides a number of the form

$$\{(t+u\sqrt{a})^{p+1} - (t-u\sqrt{a})^{p+1}\} / \sqrt{a}.$$

A. M. Legendre⁷ proved that, if $\phi^2 - A\psi^2 = 1$, then $(\phi + \psi\sqrt{A})^a - 1$ is of the form $r + s\sqrt{A}$, where r and s are divisible by a prime ω , not dividing $A\psi$, for

$$q = \omega - 1 \text{ if } \left(\frac{A}{\omega}\right) = +1, \quad q = \omega + 1 \text{ if } \left(\frac{A}{\omega}\right) = -1.$$

C. F. Gauss⁸ proved [Lagrange's⁶ result] that, if b is a quadratic non-residue of the prime p , then B_{p+1} is divisible by p for every integral value of a . If e is a divisor of $p+1$, then B_e is divisible by p for $e-1$ values of a , being a factor of B_{p+1} .

G. L. Dirichlet⁹ proved that, if b is an integer not a square and x is any integer prime to b , and if U, V are polynomials in x, b such that

$$(x + \sqrt{b})^n = U + V\sqrt{b},$$

then U and V have no common odd divisors. If n is an odd prime, no prime of which b is a quadratic residue is a factor of V unless it be of the form $2mn+1$. No prime of which b is a quadratic non-residue is a factor of V unless it be of the form $2mn-1$. Lagrange⁶ had proved conversely that a

¹Scritti, I, 1857 (Liber Abbaci), 283-4.

²L'Arithmétique de Simon Stevin de Bruges, par Albert Girard, Leyde, 1634, p. 677. Les Oeuvres Math. de Simon Stevin, 1634, p. 169.

³Phil. Trans. Roy. Soc. London, 48, I, 1753, 368-376; abridged edition, 10, 1809, 430-4.

⁴Novi Comm. Acad. Petrop., 18, 1773, 185; Comm. Arith., 1, 554.

⁵Additions to Euler's Algebra, 2, 1774, §§ 78-9, pp. 599-607. Euler, Opera Omnia, (1), 1, 619.

⁶Nouv. Mém. Ac. Berlin, année 1775 (1777), 343; Oeuvres, 3, 782-3.

⁷Théorie des nombres, 1798, p. 457; ed. 2, 1808, p. 429; ed. 3, 1830, vol. 2, Art. 443, pp. 111-2.

⁸Disq. Arith., 1801, Art. 123. ⁹Deformis linearibus, Breslau, 1827; Werke, 1, 51. Cf. Kronecker.⁵⁴

prime of which b is a non-residue, and having the form $2mn-1$, will divide V . If $b = -n$, where n is a prime $4m+3$, no prime divides V unless it is of the form $kn \equiv 1$, and conversely. The divisors of U are discussed for the case n a power of 2; in particular, of $U = x^4 + 6bx^2 + b^2$ when $n = 4$.

J. P. M. Binet¹⁰ noted that the number of terms of a solution v_n , expressed as a function of r_1, r_2, \dots , of the equation $v_{n+2} = v_{n+1} + r_n v_n$ in finite differences is

$$\frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right\}.$$

This equals U_n as shown by taking each r_n to be unity.

G. Lamé¹¹ used the series of Pisano¹ to prove that the number of divisions necessary to find the g. c. d. of two integers by the usual process of division does not exceed five times the number of digits in the smaller integer. Lionnet¹² added that the number of divisions does not exceed three times it when no remainder exceeds half the corresponding divisor. See also Serret, *Traité d'Arithmétique*; C. J. D. Hill, *Acta Univ. Lundensis*, 2, 1865, No. 1; E. Lucas, *Nouv. Corresp. Math.*, 2, 1876, 202, 214; 4, 1878, 65, and *Théorie des Nombres*, 1891, 335, Ex. 3; P. Bachmann, *Niedere Zahlentheorie*, 1902, 116-8; L. Grosschmid, *Math.-Naturwiss. Blätter*, 8, 1911, 125-7, for an elementary proof by induction; *Math. és Phys. Lapok*, 23, 1914, 5-9; R. D. Carmichael, *Theory of Numbers*, p. 24, Ex. 2.

H. Siebeck¹³ considered the recurring series defined by

$$N_r = aN_{r-1} + cN_{r-2}, \quad N_0 = 0, \quad N_1 = 1,$$

for a, c relatively prime. By induction,

$$N_r = a^{r-1} + \binom{r-2}{1} a^{r-3} c + \binom{r-3}{2} a^{r-5} c^2 + \dots + \frac{r}{2} a^\beta c^\gamma,$$

where $\beta = 0$ or 1, $\gamma = (r-1)/2$ or $(r-2)/2$, according as r is odd or even;

$$N_{rm} = r c^{r-1} N_{m-1}^{r-1} N_m N_1 + \binom{r}{2} c^{r-2} N_{m-1}^{r-2} N_m^2 N_2 + \dots + N_m^r N_r,$$

whence N_{rm} is divisible by N_m . If p and q are relatively prime, N_p and N_q are relatively prime and conversely. If p is a prime, $b = a^2 + 4c$, and $s = (b/p)$ is Legendre's symbol, then

$$N_p \equiv s, \quad N_{p-s} \equiv 0 \pmod{p},$$

so that either N_{p+1} or N_{p-1} is divisible by p .

J. Dienger¹⁴ considered the question of the number of terms of the series of Pisano with the same number of digits and the problem to find the rank of a given term.

A. Genocchi¹⁵ took a and b to be relatively prime integers and proved that B_{mn} is divisible by B_m and that the quotient Q has no odd divisor in

¹⁰*Comptes Rendus Paris*, 17, 1843, 563.

¹¹*Ibid.*, 19, 1844, 867-9. Cf. Binet, pp. 937-9.

¹²*Complément des éléments d'arithmétique*, 1857, 39-42.

¹³*Jour. für Math.*, 33, 1846, 71-6.

¹⁴*Archiv Math. Phys.*, 16, 1851, 120-4.

¹⁵*Annali di Mat.*, (2), 2, 1868-9, 256-267. Cf. Genocchi^{22, 61}.

common with B_m other than a divisor of n . If p is an odd divisor of B_m and if h is the least k for which B_k is divisible by p , then h is a divisor of m . If p is an odd prime, B_{p-1} or B_{p+1} is divisible by p according as b is a quadratic residue or non-residue of p , whatever be the value of a . This is used to prove the existence of primes of the two forms $n^2 \pm 1$ (n a prime > 2) and the existence of an infinitude of primes of each of the forms $mz \pm 1$ [Ch. XVIII].

E. Lucas¹⁶ stated without proof theorems on the series of Pisano.¹ The sum of the first n terms equals $U_{n+2} - 2$; the sum of those terms taken with alternate signs equals $(-1)^n U_{n-1}$. Also

$$U_{n-1}^2 + U_n^2 = U_{2n}, \quad U_n U_{n+1} - U_{n-1} U_{n-2} = U_{2n}, \quad U_n^3 + U_{n+1}^3 - U_{n-1}^3 = U_{3n+2}.$$

We have the symbolic formulas

$$U^{n+p} = U^{n-p}(U+1)^p, \quad U^{n-p} = U^n(U-1)^p,$$

where, after expansion, exponents are replaced by subscripts. From E. Catalan's *Manuel des Candidats à l'École Polytechnique*, I, 1857, 86, he quoted

$$U_n = \frac{n+1}{2^n} \left\{ 1 + \frac{5}{3} \binom{n}{2} + \frac{5^2}{5} \binom{n}{4} + \dots \right\}.$$

Lucas¹⁷ employed the roots a, b of $x^2 = x + 1$ and set

$$u_n = \frac{a^n - b^n}{a - b}, \quad v_n = a^n + b^n = \frac{u_{2n}}{u_n} = u_{n-1} + u_{n+1}.$$

The u 's form the series of Pisano with the terms 0, 1 prefixed, so that $u_0 = 0, u_1 = u_2 = 1, u_3 = 2$. Since $5u_n^2 - v_n^2 = \pm 4$, u_n and v_n have no common factor other than 2. If p is a prime $\neq 2, 5$, we have $u_p \equiv \pm 1, v_p \equiv 1 \pmod{p}$. We have the symbolic formulas

$$u_{n+2kp} = u^n \{ v_k u^k - (-1)^k \}^p, \quad (-1)^{kp} u_{n-kp} = u^n \{ v_k - u^k \}^p.$$

Given a law $U_{n+k} = A_0 U_{n+p} + \dots + A_p U_n$ of recurrence, we can replace the symbol U^k by $\phi(U)$, where

$$\phi(u) = A_0 u^p + A_1 u^{p-1} + \dots + A_{p-1} u + A_p,$$

since $U_{n+kp} = U^n \{ \phi(U) \}^p$, symbolically.

E. Lucas¹⁸ stated theorems on the series of Pisano. We have

$$2^n \sqrt{5} u_n = (1 + \sqrt{5})^n - (1 - \sqrt{5})^n, \quad u_{n+1} = 1 + \binom{n}{1} + \binom{n-1}{2} + \dots,$$

and his¹⁶ symbolic formulas with u 's in place of U 's. u_{pq} is divisible by u_p and u_q , and by their product if p, q are relatively prime. Set $v_n = u_{2n}/u_n$. Then

$$v_{n+2} = v_{n+1} + v_n, \quad v_{4n} = v_{2n}^2 - 2, \quad v_{4n+2} = v_{2n+1}^2 + 2.$$

¹⁶Nouv. Corresp. Math., 2, 1876, 74-5.

¹⁷*Ibid.*, 201-6.

¹⁸Comptes Rendus Paris, 82, 1876, 165-7.

If the term of rank $A+1$ in Pisano's series is divisible by the odd number A of the form $10p \pm 3$ and if no term whose rank is a divisor of $A+1$ is divisible by A , then A is a prime. If the term of rank $A-1$ is divisible by $A=10p \pm 1$ and if no term of rank a divisor of $A-1$ is divisible by A , then A is a prime. It is stated that $A=2^{127}-1$ is a prime since $A=10p-3$ and u_k is never divisible by A for $k=2^n$, except for $n=127$.

Lucas¹⁹ employed the roots a, b of a quadratic equation $x^2 - Px + Q = 0$, where P, Q are relatively prime integers. Set

$$u_n = \frac{a^n - b^n}{a - b}, \quad v_n = a^n + b^n, \quad \delta = a - b.$$

The quotients of $\delta u_n \sqrt{-1}$ and v_n by $2Q^{n/2}$ are functions analogous to the sine and cosine. It is stated that

$$\begin{aligned} (1) \quad & u_{2n} = u_n v_n, & v_n^2 - \delta^2 u_n^2 &= 4Q^n, \\ (2) \quad & 2u_{m+n} = u_m v_n + u_n v_m, & u_n^2 - u_{n-1} u_{n+1} &= Q^{n-1}. \end{aligned}$$

Not counting divisors of Q or δ^2 , we have the theorems:

(I) u_{pq} is divisible by u_p, u_q , and by their product if p, q are relatively prime.

(II) u_n, v_n are relatively prime.

(III) If d is the g. c. d. of m, n , then u_d is the g. c. d. of u_m, u_n .

(IV) For n odd, u_n is a divisor of $x^2 - Qy^2$.

By developing u_{np} and v_{np} in powers of u_n and v_n , we get formulas analogous to those for $\sin nx$ and $\cos nx$ in terms of $\sin n$ and $\cos n$, and thus get the law of apparition of primes in the recurring series of the u_n [stated explicitly in Lucas²⁰], given by Fermat when δ is rational and by Lagrange when δ is irrational. The developments of u_n^p and v_n^p as linear functions of u_n, u_{2n}, \dots are like the formulas of de Moivre and Bernoulli for $\sin^p x$ and $\cos^p x$ in terms of $\sin kx, \cos kx$. Thus—

(V) If n is the rank of the first term u_n containing the prime factor p to the power λ , then u_{pn} is the first term divisible by $p^{\lambda+1}$ and not by $p^{\lambda+2}$; this is called the law of repetition of primes in the recurring series of u_n .

(VI) If p is a prime $4q+1$ or $4q+3$, the divisors of u_{pn}/u_n are divisors of $x^2 - py^2$ or $\delta^2 x^2 + py^2$, respectively.

(VII) If $u_{p \pm 1}$ is divisible by p , but no term of rank a divisor of $p \pm 1$ is divisible by p , then p is a prime.

Lucas²⁰ proved the theorems stated in the preceding paper. Theorems II and IV follow from (1₂) and (2₂), while (2₁) shows that every factor common to u_{m+n} and u_m divides u_n and conversely.

(VIII) If a and b are irrational, but real, u_{p+1} or u_{p-1} is divisible by the prime p , according as δ^2 is a quadratic non-residue or residue of p (law of apparition of primes in the u 's). If a and b are integers, u_{p-1} is divisible by p . Hence the proper divisors of u_n are of the form $kn+1$ if δ is rational, $kn \pm 1$ if δ is irrational.

¹⁹Comptes Rendus Paris, 82, 1876, pp. 1303-5.

²⁰Sur la théorie des nombres premiers, Atti R. Accad. Sc. Torino (Math.), 11, 1875-6, 928-937.

The law V of repetition of primes follows from

$$\delta^{p-1}u_n^p = u_{pn} - Q^n \binom{p}{1} u_{(p-2)n} + Q^{2n} \binom{p}{2} u_{(p-4)n} - \dots \pm Q^{tn} \binom{p}{t} u_n,$$

where $t = (p-1)/2$. Special cases of the law are due to Arndt,³³ p. 260, and Sancery,⁶¹ each quoted in Ch. VII. Theorem VII, which follows from VIII, gives a test for the primality of $2^n \pm 1$ which rests on the success of the operation, whereas Euler's test for $2^{31} - 1$ was based on the failure of the operation. The work to prove that $2^{31} - 1$ is prime is given, and it is stated that $2^{67} - 1$ was tested and found composite,²¹ contrary to Mersenne. Finally, $x^2 + Qy^2$ is shown to have an infinitude of prime divisors.

A. Genocchi²² noted that Lucas' u_n, v_n are analogous to his¹⁵ B_n, A_n . [If we set $\alpha = a + \sqrt{b}$, $\beta = a - \sqrt{b}$, we have

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} = B_k, \quad v_k = \alpha^k + \beta^k = 2A_k.]$$

Lucas²³ stated that, if $4m+3$ is prime, $p = 2^{4m+3} - 1$ is prime if the first term of the series 3, 7, 47, . . ., defined by $r_{n+1} = r_n^2 - 2$, which is divisible by p is of rank $4m+2$; but p is composite if no one of the first $4m+2$ terms is divisible by p . Finally, if α is the rank of the first term divisible by p , the divisors of p are of the form $2^ak \pm 1$, together with the divisors of $x^2 - 2y^2$. There are analogous tests by recurring series for the primality of

$$3 \cdot 2^{4m+3} - 1, \quad 2 \cdot 3^{4m+2} \pm 1, \quad 2 \cdot 3^{4m+3} - 1, \quad 2 \cdot 5^{2m+1} + 1.$$

Lucas²⁴ proposed as an exercise the determination of the last digit in the general term of the series of Pisano and for the series defined by $u_{n+2} = au_{n+1} + bu_n$; also the proof of VIII: If p is a prime,

$$u_{p-1} = \frac{(a + \sqrt{b})^{p-1} - (a - \sqrt{b})^{p-1}}{\sqrt{b}}$$

is divisible by p if b is a quadratic residue of p , excepting values of a for which $a^2 - b$ is divisible by p ; and the corresponding result [of Lagrange⁶ and Gauss⁸] for u_{p+1} . Moret-Blanc²⁵ gave a proof by use of the binomial theorem and omission of multiples of p .

Lucas²⁶ wrote s_n for the sum of the n th powers of the roots of an equation whose coefficients are integers, the leading one being unity. Then $s_{np} - s_n^p$ is an integral multiple of p . Take $n = 1$. Then $s_1 = 0$ implies $s_p \equiv 0 \pmod{p}$. It is stated that if $s_1 = 0$ and if s_k is divisible by p for $k = p$, but not for $k < p$, then p is a prime.

²¹A. Cunningham, Proc. Lond. Math. Soc., 27, 1895-6, 54, remarked that, while primality is proved by Lucas' process by the success of the procedure, his verification that a number is composite is indirect and proved by the failure of the process and hence is liable to error.

²²Atti. R. Accad. Sc. Torino, 11, 1875-6, 924.

²³Comptes Rendus Paris, 83, 1876, 1286-8.

²⁴Nouv. Ann. Math., (2), 15, 1876, 82.

²⁵Ibid., (2), 20, 1881, 258 [p. 263, for primality of $2^{31} - 1$].

²⁶Assoc. franç. avanc. sc., 5, 1876, 61-67. Cf. Lucas³³.

By use of (1) and (2), theorems I–IV are proved. Theorem VIII is stated, and VII is proved. Employing two diagrams and working to base 2, he showed that $2^{31} - 1$ is a prime.

Lucas²⁷ considered a product $m = p^{\omega} r^{\rho} \dots$ of powers of primes, no one dividing Q . Set $\Delta = (a-b)^2$, $(\Delta/p) = 0, \pm 1 \equiv \Delta^{(p-1)/2} \pmod{p}$,

$$\psi(m) = p^{\omega-1} r^{\rho-1} \dots \left[p - \left(\frac{\Delta}{p} \right) \right] \left[r - \left(\frac{\Delta}{r} \right) \right] \dots$$

Then $u_t \equiv 0 \pmod{m}$ for $t = \psi(m)$. The ranks n of terms u_n divisible by m are multiples of a certain divisor μ of $\psi(m)$. This μ is the exponent to which a or b belongs modulo m . The case $b=1$ gives Euler's generalization of Fermat's theorem. The primality test²³ is reproduced and applied to show that $2^{19} - 1$ is a prime.

Lucas²⁸ considered the series of Pisano. Taking $a, b = (1 \pm \sqrt{5})/2$, we have $u_1 = u_2 = 1, u_3 = 2$, etc. According as n is odd or even the divisors of u_{3n}/u_n are divisors of $5x^2 - 3y^2$ or $5x^2 + 3y^2$; those of u_{4n}/u_{2n} are divisors of $5x^2 - 2y^2$ or $5x^2 + 2y^2$; those of v_{3n}/v_n are divisors of $x^2 + 3y^2$ or $x^2 - 3y^2$; those of v_{2n} are divisors of $x^2 + 2y^2$ or $x^2 - 2y^2$; those of u_{2n}/u_n are divisors of $x^2 + 5y^2$ or $x^2 - 5y^2$. The law V of repetition of primes and theorem III are stated. The law VIII of apparition of primes now takes the following form: If p is a prime $10q \pm 1$, u_{p-1} is divisible by p ; if p is a prime $10q \pm 3$, u_{p+1} is divisible by p . The test¹⁸ for the primality of A is given and applied to show that $2^{127} - 1$ and $2^{31} - 1$ are primes. There is a table of prime factors of u_n for $n \leq 60$. Finally, $4u_{pn}/u_n$ is expressible in the form $x^2 - py^2$ or $5x^2 + py^2$ according as the prime p is of the form $4q+1$ or $4q+3$.

Lucas²⁹ considered the series defined by $r_{n+1} = r_n^2 - 2$,

$$\sqrt{5}r_1 = \left(\frac{1+\sqrt{5}}{2} \right)^A - \left(\frac{1-\sqrt{5}}{2} \right)^A, \quad r_2 = \left(\frac{1+\sqrt{5}}{2} \right)^A + \left(\frac{1-\sqrt{5}}{2} \right)^A.$$

Let $A \equiv 3$ or $9 \pmod{10}$, $q \equiv 0 \pmod{4}$; or $A \equiv 7, 9 \pmod{10}$, $q \equiv 1 \pmod{4}$; or $A \equiv 1, 7 \pmod{10}$, $q \equiv 2 \pmod{4}$; or $A \equiv 1, 3 \pmod{10}$, $q \equiv 3 \pmod{4}$. Then $p = 2^q A - 1$ is a prime if the rank of the first term divisible by p is q ; if a ($a < q$) is the rank of the first term divisible by p , the divisors of p are either of the form* $2aAk+1$, or of the forms of the divisors of $x^2 - 2y^2$ and $x^2 - 2Ay^2$. Corresponding tests are given for $2^q A + 1$ and $3^q A - 1$. The first part of the theorem of Pepin³⁰ for testing the primality of $a_n = 2^{2^n} + 1$ follows from theorem VII with $a=5, b=1, p=a_n$; the second part follows from the reciprocity theorem and the form of $a_n - 1$.

For $A=p$, let the above r_1 become r . When $p \equiv 7$ or $9 \pmod{10}$ and p is a prime, then $2p-1$ is a prime if and only if $r \equiv 0 \pmod{2p-1}$. When $p = 4q+3$ is a prime, $2p+1$ is a prime if and only if $2^p \equiv 1 \pmod{2p+1}$. When $p = 4q+3$ is a prime, $2p-1$ is a prime if and only if

²⁷Comptes Rendus Paris, 84, 1877, 439–442. Corrected by Carmichael.³⁹

²⁸Bull. Bibl. Storia Sc. Mat. e Fis., 10, 1877, 129–170. Reprinted as "Recherches sur plusieurs ouvrages de Léonard de Pise." Cf. von Sterneck²¹ of Ch. XIX.

²⁹Assoc. franç. avanc. sc., 6, 1877, 159–166. *Corrected to $2^a A k \equiv 1$ in Lucas³⁹; see Lucas.⁴²

³⁰Comptes Rendus Paris, 85, 1877, 329–331. See Ch. XV, Pepin¹⁹, Lucas,^{18, 22} Proth.²³

$$\frac{1}{\sqrt{2}}\{(1+\sqrt{2})^p - (1-\sqrt{2})^p\} \equiv 0 \pmod{2p-1}.$$

To test the primality of $p = 2^{4q+1} - 1$, use $x^2 - 4x + 1 = 0$ with the roots $2 \pm \sqrt{3}$. Then if p is a prime, u_{p+1} is divisible by p . We use the residues of the series 2, 7, 97, ... defined by $r_{n+1} = 2r_n^2 - 1$.

Lucas³¹ stated that $p = 2^{4m+3} - 1$ is a prime if the rank of the first term²³ of 3, 7, 47, ... divisible by p is between $2m$ and $4m+2$. To test $P = 2^{4q+1} - 1$, form the series

$$r_1 = 1, \quad r_2 = -1, \quad r_3 = -7, \quad r_4 = 17, \dots, \quad r_{n+1} = 2r_n^2 - 3^{2^{n-1}};$$

if l is the least integer for which r_l is divisible by P , then P is a prime when l is comprised between $2q$ and $4q+1$, composite when $l > 4q+1$.

Lucas³² expressed u_n, v_n as polynomials in P and $\Delta = P^2 - 4Q = \delta^2$, obtained various relations between them corresponding to relations between sine and cosine; in particular,

$$u_{n+2} = Pu_{n+1} - Qu_n, \quad u_{n+2r} = v_r u_{n+r} - Q^r u_n,$$

and formulas derived from them by replacing u by v ; also symbolic formulas generalizing those¹⁶ for the series of Pisano.

In the second paper, u_{n+1}, v_n are expressed as determinants of order n whose elements are $Q, -P, 2, 1, 0$. There is given a continued fraction for $u_{(n+1)r}/u_{nr}$, from which is derived (1₂) and generalizations. The same fraction is developed into a series of fractions.

Lucas³³ noted that u_{nr} is divisible by u_r since

$$\frac{u_{nr}}{u_r} = v_{(n-1)r} + Q^r v_{(n-3)r} + Q^{2r} v_{(n-5)r} + \dots + Q^{tr} v_r,$$

where $t = \frac{1}{2}n - 1$ if n is even, $t = \frac{1}{2}(n-1)$ if n is odd, the final factor being then absent. Proof is given for (2₁) and $2v_{m+n} = v_m v_n + \Delta u_n u_m$. From these are derived new formulas by changing the sign of n and applying

$$u_{-n} = -u_n/Q^n, \quad v_{-n} = v_n/Q^n.$$

To show that

$$[m, n] = \frac{u_{m+n} u_{m+n-1} \dots u_{m+1}}{u_n u_{n-1} \dots u_1}$$

is integral, apply (2₁) repeatedly to get

$$2[m, n] = [m-1, n]v_n + [m, n-1]v_m.$$

Finally, sums of squares of functions u_n, v_n are found.

Lucas³⁴ gave a table of the linear forms $4\Delta + r$ of the odd divisors of $x^2 + \Delta y^2$ and $x^2 - \Delta y^2$ for $\Delta = 1, \dots, 30$. By use of (1₂), it is shown that the terms of odd rank in the series u_n are divisors of $x^2 - Qy^2$; the terms of even or odd rank in the series v_n are divisors of $x^2 + \Delta y^2$ or $x^2 + Q\Delta y^2$, respectively.

³¹Messenger Math., 7, 1877-8, 186.

³²Sur la théorie des fonctions numériques simplement périodiques, Nouv. Corresp. Math., 3, 1877, 369-376, 401-7. These and the following five papers were reproduced by Lucas.³³

³³Ibid., 4, 1878, 1-8, continuation of preceding.

³⁴Ibid., pp. 33-40.

Lucas³⁵ proved III by use of (2₁) and gave

$$u_{n+1} = \phi_n u_1 - Q \phi_{n-1} u_0,$$

$$\phi_n = P^n - \binom{n-1}{1} P^{n-2} Q + \binom{n-2}{2} P^{n-4} Q^2 - \binom{n-3}{3} P^{n-6} Q^3 + \dots;$$

$$u_{np} = \delta^{p-1} u_n^p + p Q^n \delta^{p-3} u_n^{p-2} + \frac{p(p-3)}{2} Q^{2n} \delta^{p-5} u_n^{p-4} + \dots$$

Lucas³⁶ determined the quadratic forms of divisors of v_{2n} from

$$v_{2n} = \Delta u_n^2 + 2Q^n, \quad v_{2n} = v_n^2 - 2Q^n.$$

In the last, take $Q = 2q^2$, $n = 2\mu + 1$; thus $v_{4\mu+2}$ factors if Q is the double of a square. As a special case we have the result by H. LeLasseur (p. 86):

$$2^{2(2q+1)} + 1 = (2^{2q+1} + 2^{q+1} + 1)(2^{2q+1} - 2^{q+1} + 1).$$

In the first expression for v_{2n} , take $n = \mu + 1$, $\Delta = \pm 2h^2$, $Q = \mp g^2$; thus $v_{4\mu+2}$ factors when $Q\Delta$ is of the form $-2t^2$. Similarly, $v_{4\mu}$ factors if $\Delta = -2t^2$.

Lucas³⁷ gave the formulas

$$\frac{u_{3n}}{u_n} = \Delta u_n^2 + 3Q^n, \quad \frac{v_{3n}}{v_n} = v_n^2 - 3Q^n,$$

developments of u_n^p , v_n^p as linear functions of v_{kn} , $k = p, p-2, p-4, \dots$, and complicated developments of u_{nr} , v_{nr} .

Lucas³⁸ reproduced the preceding series of seven papers, added (p. 228) a theorem on the expression of $4u_{pr}/u_r$ as a quadratic form, a proof (p. 231) of his²⁶ test for primality by use of the s_t , and results on primes and perfect numbers cited elsewhere.

Lucas³⁹ considered series u_n of the first kind (in which the roots a, b are relatively prime integers) and deduced Fermat's theorem and the analogue $u_t \equiv 0 \pmod{m}$, $t = \phi(m)$, of Euler's generalization. Proof is given of the earlier theorems VII, VIII and (p. 300) of his²⁷ generalization of the Euler-Fermat theorem. The primality test²³ is stated (p. 305) and applied to show that $2^{31} - 1$ and $2^{19} - 1$ are primes. It is stated (page 309) that $p = 2^{4q+3} - 1$ is prime if and only if

$$3 \equiv 2 \cos \pi/2^{2q+1} \pmod{p},$$

after rationalizing with respect to the radicals in the value of the cosine. The primality tests²⁹ are given (page 310), with similar ones for $3^q A + 1$, $2 \cdot 5^q A + 1$. The tests²⁹ for the primality of $2p + 1$ are given (p. 314). The primality test²⁹ for $2^{4q+1} - 1$ is proved (pp. 315-6).

Lucas⁴⁰ reproduced his³⁶ earlier results, and for $p = 3, 5, 7, 11, 13, 17$, expressed v_{pr}/v_{2r} in the form $x^2 - 2pQ^r y^2$, and, for p a prime ≤ 31 , expressed

³⁵Nouv. Corresp. Math., 4, 1878, 65-71.

³⁶Ibid., pp. 97-102.

³⁷Ibid., pp. 129-134, 225-8.

³⁸Amer. Jour. Math., 1, 1878, 184-220. Errors noted by Carmichael.³⁹

³⁹Ibid., pp. 289-321.

⁴⁰Atti R. Accad. Sc. Torino, 13, 1877-8, 271-284.

u_{pr}/u_r in the form $\Delta x^2 \pm pQ^ry^2$. The prime factors of $3^{29} \pm 1$ are given on p. 280. The proper divisors of $2^{4n} + 1$ are known to be of the form $8nq + 1$; it is shown that q is even. Thus for $2^{32} + 1$ the first divisor to be tried is 641, for $2^{12} + 1$ the first one is 114689; in each case the division is exact (cf. Ch. XV). The following is a generalization: If the product of two relatively prime integers a and b is of the form $4h + 1$, the proper divisors of $a^{2abn} + b^{2abn}$ are of the form $8abnq + 1$. A primality test for $2^{4q+3} - 1$ is given. Finally, $p = 2^{4nq+2n+1} - 1$ is a prime if and only if

$$\left(2^n + \sqrt{2^{2n} + 1}\right)^{\frac{p+1}{2}} + \left(2^n - \sqrt{2^{2n} + 1}\right)^{\frac{p+1}{2}} \equiv 0 \pmod{p}.$$

T. Pepin⁴¹ gave a test for the primality of $q = 2^n - 1$. Let

$$u_1 \equiv \frac{2(a^2 - b^2)}{a^2 + b^2} \pmod{q}$$

and form the series u_1, u_2, \dots, u_{n-1} by use of

$$u_{a+1} \equiv u_a^2 - 2 \pmod{q}.$$

Then q is a prime if and only if u_{n-1} is divisible by q . This test differs from that by Lucas²³ in the choice of u_1 .

E. Lucas⁴² reproduced his²⁹ test for the primality of $2^q A - 1$, etc., and the test at the end of another paper,⁴⁰ with similar tests for $2^{4q+3} - 1$ and $2^{12q+5} - 1$.

G. de Longchamps⁴³ noted that, if $d_k = u_k - au_{k-1}$,

$$d_p = b^{p-1}, \quad d_p d_q = b^{p+q-2},$$

with the generalization

$$\prod_{j=1}^x d_{p_j} = d_s, \quad s = p_1 + \dots + p_x - x + 1.$$

Take $p_1 = \dots = p_x = p$. Hence

$$(u_p - au_{p-1})^x = u_{px-x+1} - au_{px-x}.$$

There is a corresponding theorem for the v 's.

J. J. Sylvester⁴⁴ considered the g. c. d. of u_x, u_{x+1} if

$$u_x = (2x - 1)u_{x-1} - (x - 1)u_{x-2}.$$

E. Gelin⁴⁵ stated and E. Cesàro⁴⁶ proved by use of $U_{n+p} = U_p U_n + U_{p-1} U_{n-1}$ that, in the series of Pisano, the product of the means of four consecutive terms differs from the product of the extremes by ± 1 ; the fourth power of the middle term of five consecutive terms differs from the product of the other four terms by unity.

⁴¹Comptes Rendus Paris, 86, 1878, 307-310.

⁴²Bull. Bibl. Storia Sc. Mat. e Fis., 11, 1878, 783-798. The further results are cited in Ch. XVI. Comptes Rendus, 90, 1880, 855-6, reprinted in Sphinx-Oedipe, 5, 1910, 60-1.

⁴³Nouv. Corresp. Math., 4, 1878, 85; errata, p. 128.

⁴⁴Comptes Rendus Paris, 88, 1879, 1297; Coll. Papers, 3, 252.

⁴⁵Nouv. Corresp. Math., 6, 1880, 384.

⁴⁶Ibid., 423-4.

Magnon,⁴⁷ in reply to Lucas, proved that

$$\frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3} - \dots = \frac{2}{1 - \sqrt{5}},$$

if $a_n - 1$ is the sum of the squares of the first $n - 1$ terms of Pisano's series.

H. Brocard⁴⁸ studied the arithmetical properties of the U 's defined by $U_{n+1} = U_n + 2U_{n-1}$, $U_0 = 1$, $U_1 = 3$, in connection with the n th pedal triangle.

E. Cesàro⁴⁹ noted that if U_n is the n th term of Pisano's series, then $(2U+1)^n - U^{3n} = 0$, symbolically.

E. Lucas⁵⁰ gave his²³ test for the primality of $2^{4q+3} - 1$.

A. Genocchi⁵¹ reproduced his¹⁵ results.

M. d'Ocagne⁵² proved for Pisano's series that [Lucas¹⁶]

$$\sum_{i=0}^p u_i = u_{p-2} - 1, \quad \Sigma (-1)^i u_i = (-1)^p u_{p-1} - 1, \quad \lim_{p \rightarrow \infty} \frac{u_p}{u_{p-i}} = \left(\frac{1 + \sqrt{5}}{2} \right)^i,$$

$$u_p u_i - u_{p+1} u_{i-1} = (-1)^{i+1} u_{p-i+1}, \quad u_p u_{p-1} = u_p^2 - u_{p-1}^2 + (-1)^p.$$

The main problem treated is that to insert p terms a_1, \dots, a_p between two given numbers $a_0 = a$, $a_{p+1} = b$, such that $a_i = a_{i-1} + a_{i-2}$. The solution is

$$a_i = \frac{bu_i + (-1)^i au_{p+1-i}}{u_{p+1}}.$$

Most of the paper is devoted to the question of the maximum number of negative terms in the series of a 's.

E. Catalan^{52a} proved that $U_n^2 - U_{n-p}U_{n+p} = (-1)^{n-p+1}U_{p-1}^2$ for Pisano's series.

E. Lucas⁵³ stated, apropos of sums of squares, that

$$u_{2n+1} = u_{n+1}^2 + u_n^2, \quad v_{2n} = u_{n-1}^2 + 2u_n^2 + u_{n+1}^2,$$

$$v_{4n+2} = v_{2n+1}^2 + 2, \quad v_{4n} = (2u_n)^2 + u_{n+1}^2 + 2.$$

L. Kronecker⁵⁴ obtained Dirichlet's⁹ theorems by use of modular systems.

Lucas^{54a} proved that, if $u_n = (a^n - b^n)/(a - b)$,

$$\frac{u_n^n - u_{(p-1)n}}{u_{p-1}}$$

is divisible by u_p when p is a prime and n is odd and not divisible by p , and by u_p^2 when $n = 2p + 1$.

L. Liebethuth⁵⁵ considered the series $P_1 = 1$, $P_2 = x$, \dots , $P_n = xP_{n-1} - P_{n-2}$, and proved any two consecutive terms are relatively prime, and

$$P_n = P_\lambda P_{n-\lambda+1} - P_{\lambda-1} P_{n-\lambda} \quad (\lambda < n).$$

Taking $n = 2\lambda$, 3λ , \dots , we see that P_λ is a common factor of $P_{2\lambda}$, $P_{3\lambda}$, \dots .

The g. c. d. of P_m , P_n is P_d , where d is the g. c. d. of m , n . Next,

⁴⁷Nouv. Corresp. Math., 6, 1880, 418-420.

⁴⁸Nouv. Corresp. Math., 6, 1880, 145-151.

⁴⁹*Ibid.*, 528; Nouv. Ann. Math., (3), 2, 1883, 192; (3), 3, 1884, 533. *Journ. de Sc. Math.* Astr., 6, 1885, 17.

⁵⁰Récréations mathématiques, 2, 1883, 230.

⁵¹Comptes Rendus Paris, 98, 1884, 411-3.

⁵²Bull. Soc. Math. France, 14, 1885-6, 20-41.

^{52a}Mém. soc. roy. sc. Liège, (2), 13, 1886, 319-21 (= *Mélanges Math.*, II).

⁵³Mathesis, 7, 1887, 207; proofs, 9, 1889, 234-5.

⁵⁴Berlin Berichte, 1888, 417-423; Werke, 3, I, 281-292. Cf. Kronecker³⁸ of Ch. XVI.

^{54a}Assoc. franç. avanc. sc., 1888, II, 30.

⁵⁵Beitrag zur Zahlentheorie, Progr., Zerbst, 1888.

$$P_1 + P_3 + \dots + P_{2n-1} = P_n^2, \quad P_2 + P_4 + \dots + P_{2n} = P_n P_{n+1}.$$

If $P_n \equiv P_m \pmod{P_\lambda}$ then $n \equiv m \pmod{2\lambda}$. Also,

$$P_n = x^{n-1} + \sum_{k=1}^n (-1)^k \frac{(n-k-1) \dots (n-2k)}{1 \cdot 2 \dots k} x^{n-2k-1}.$$

If a_n/b_n is the n th convergent to $\frac{1}{x} - \frac{1}{x} + \frac{1}{x} - \dots$, then $a_{n+2} = xa_{n+1} - a_n$, $b_n = a_{n+1}$. Hence $a_n = P_n$ if $a_1 = 1$, $a_2 = x$.

Sylvester stated and W. S. Foster^{55a} proved that if $f(\theta)$ is a polynomial with integral coefficients and $u_{x+1} = f(u_x)$, $u_1 = f(0)$, and δ is the g. c. d. of r, s , then u_δ is the g. c. d. of u_r, u_s .

A. Schönflies⁵⁶ considered the numbers $n_0 = 1, n_1, \dots, n_q$ defined by

$$n_\lambda = n^\lambda - n^{\lambda-1} + n^{\lambda-2} - \dots + (-1)^\lambda \quad (\lambda = 0, 1, \dots)$$

and proved geometrically that if n_{r-1} is the least of these numbers which has a common factor with n_q , then r is a divisor of $q+1$, while a relation

$$mn_i \equiv mn_{r+i} \pmod{n_q}$$

holds for every index i .

L. Gegenbauer⁵⁷ gave a purely arithmetical proof of this theorem.

E. Lucas⁵⁸ gave an exposition of his theory, with an introduction to recurring series.

M. Frolov⁵⁹ used a table of quadratic residues of composite numbers to factor Lucas' numbers v_n .

D. F. Seliwanov⁶⁰ proved Lucas' results on the factors of u_n, v_n .

E. Catalan⁶¹ gave the first 43 terms of the series of Pisano, noted that U_n divides U_{2n+1} , that U_{2n} is a sum of two squares, and treated the series

$$u_n = au_{n-1} + u_{n-2}, \quad u_1 = a, \quad u_2 = a^2 + 1.$$

Fontès^{61a} proved theorems stated by Lucas⁵⁸ (p. 127), and found in an elementary way the general term of Pisano's series, as given by Binet¹¹.

E. Maillet^{61b} proved that a necessary condition that every positive integer, exceeding a certain limit, shall equal (up to a limited number of units) the sum of the absolute values of a finite number of terms of a recurring series, satisfying an irreducible law of recurrence with integral coefficients, is that all the roots of the corresponding generating equation be roots of unity.

W. Mantel⁶² noted that, if the denominator $F(x)$ of the generating fraction of a recurring series is irreducible modulo p , a prime, the residues modulo p of the terms of the recurring series repeat periodically, and the length of a period is at most $p^n - 1$; the proof is by use of Galois' generalization of Fermat's theorem. The case of a reducible $F(x)$ is also treated.

^{55a}Math. Quest. Educ. Times, 50, 1889, 54-5.

⁵⁶Math. Annalen, 35, 1890, 537.

⁵⁷Denkschriften Ak. Wiss. Wien (Math.), 57, 1890, 528.

⁵⁸Théorie des nombres, 1891, 299-336; 30; 127, ex. 1. A pamphlet, published privately by Lucas in 1891, is cited in l'intermédiaire des math., 5, 1898, 58.

⁵⁹Assoc. franç. avanc. sc., 21, 1892, 149.

⁶⁰Math. Soc. Moscow, 16, 1892, 469-482 (in Russian).

⁶¹Mém. Acad. R. Belgique, 45, 1883; 52, 1893-4, 11-14.

^{61a}Assoc. franç. avanc. sc., 1894, II, 217-221.

^{61b}Assoc. franç. avanc. sc., 1896, II, 78-89

⁶²Nieuw Archief voor Wiskunde, Amsterdam, 1, 1895, 172-184.

R. W. D. Christie⁶³ stated that, for the recurring series defined by $a_{n+1} = 3a_n - a_{n-1}$, $2m-1$ is a prime if and only if $a_m - 1$ is divisible by $2m-1$. The error of this test was pointed out by E. B. Escott.⁶⁴

S. Réalis^{64a} noted that two of N consecutive terms of $7, 13, 25, \dots, 3(n^2 + n) + 7, \dots$ are divisible by N if N is a prime $6m+1$.

C. E. Bickmore^{64b} discussed factors of u_n in the final series of Catalan⁶¹. He^{64c} and others gave known formulas and properties of Pisano's series.

R. Perrin⁶⁵ employed $v_n = v_{n-2} + v_{n-3}$, $v_0 = 3$, $v_1 = 0$, $v_2 = 2$. Then v_n is divisible by n if n is a prime. This was verified to be not true when n is composite for a wide range of values of n . The same subject was considered by E. Malo⁶⁶ and E. B. Escott⁶⁷ who noted that Perrin's test is incomplete.

Several^{67a} discussed the computation of Pisano's u_n for large n 's.

E. B. Escott^{67b} computed $\Sigma 1/u_n$. E. Landau^{67c} had evaluated $\Sigma 1/u_{2h}$ in terms of the sum of Lambert's⁷ series of Ch. X, and $\Sigma 1/u_{2h+1}$ in relation to theta series.

A. Tagiuri⁶⁸ employed the series $u_1 = 1$, $u_2 = 1$, $u_3 = 2, \dots$ of Leonardo and the generalization U_1, U_2, \dots , where $U_n = U_{n-1} + U_{n-2}$, with $U_1 = a$, $U_2 = b$ both arbitrary. Writing e for $a^2 + ab - b^2$, it is proved that

$$U_{n+s} = u_{s+1}U_n + u_sU_{n-1}, \quad U_n^2 - U_{n-k}U_{n+k} = (-1)^{n-k}u_k^2e,$$

$$U_nU_s - U_{n-k}U_{s+k} = (-1)^{n-k}u_ku_{k+s-n}e.$$

$\{U_{n+s} + (-1)^sU_{n-s}\}/U_n$ is an integer independent of a, b, n ; it equals $u_{s+1} + u_{s-1}$. It is shown that u_r is a multiple of u_s if and only if r is a multiple of s .

Tagiuri⁶⁹ obtained analogous results for the series defined by $V_n = hV_{n-1} + lV_{n-2}$, and the particular series v_n obtained by taking $v_1 = 1$, $v_2 = h$. If h and l are relatively prime, v_r is a multiple of v_s if and only if r is a multiple of s . Let $\Phi(v_i)$ be the number of terms of the series of v 's which are $\leq v_i$ and prime to it; if $h > 1$, $\Phi(v_i)$ is Euler's $\phi(i)$; but, if $h = 1$, $\Phi(v_i) = \phi(i) + \phi(i/2)$, the last term being zero if i is odd. If i and j are relatively prime, $\Phi(v_{ij}) = \Phi(v_i)\Phi(v_j)$.

Tagiuri⁷⁰ proved that, for his series of v 's, the terms between v_{kp} and $v_{k(p+1)}$ are incongruent modulo v_k if $h > 1$, and for $h = 1$ except for $v_{kp+1} \equiv v_{kp+2}$. If μ is not divisible by k and ϵ is the least solution of $l^{2k\epsilon} \equiv 1 \pmod{v_k}$, then

$$v_x \equiv v_\mu \pmod{v_k} \quad \text{if } x \equiv \mu \pmod{4k\epsilon}.$$

If μ is not divisible by k , and k is odd, and ϵ_1 is the least positive solution of $l^{2k\epsilon_1} \equiv 1 \pmod{v_k}$, then $v_x \equiv v_\mu \pmod{v_k}$ if $x \equiv \mu \pmod{2k\epsilon_1}$.

A. Emmerich⁷¹ proved that, in the series of Pisano,

⁶³Nature, 56, 1897, 10.

⁶⁴Math. Quest. Educat. Times, 3, 1903, 46; 4, 1903, 52

^{64a}Math. Quest. Educat. Times, 66, 1897, 82-3; cf. 72, 1900, 40, 71.

^{64b}*Ibid.*, 71, 1899, 49-50.

^{64c}*Ibid.*, 111; 4, 1903, 107-8; 9, 1906, 55-7.

⁶⁵L'intermédiaire des math., 6, 1899, 76-7.

⁶⁶*Ibid.*, 7, 1900, 281, 312.

⁶⁷L'intermédiaire des math., 8, 1901, 63-64.

^{67a}*Ibid.*, 7, 1900, 172-7.

^{67b}*Ibid.*, 9, 1902, 43-4.

^{67c}Bull. Soc. Math. France, 27, 1899, 198-300.

⁶⁸Periodico di Mat., 16, 1901, 1-12.

⁶⁹Periodico di Mat., 97-114.

⁷⁰*Ibid.*, 17, 1902, 77-88, 119-127.

⁷¹Mathesis, (3), 1, 1901, 98-9.

$$u_{n+5} \equiv u_n \pmod{2}, \quad u_{n+5} \equiv 3u_n \pmod{5}, \quad u_{n+60} \equiv u_n \pmod{10},$$

so that $u_0, u_3, u_6, u_9, \dots$ alone are even, u_0, u_5, u_{10}, \dots are multiples of 5.

J. Wasteels⁷² proved that two positive integers x, y , for which $y^2 - xy - x^2$ equals $+1$ or -1 , are consecutive terms of the series of Pisano. If $5x^2 \pm 4$ is a square, x is a term of the series of Pisano. These are converses of theorems by Lucas.¹⁷

G. Candido⁷³ treated u_n, v_n , by algebra and function-theory.

E. B. Escott⁷⁴ proved the last result in Lucas' paper.⁴⁰

A. Arista⁷⁵ expressed $\sum_{n=1}^{\infty} u_n^{-1}$ in finite form.

M. Cipolla⁷⁶ gave extensive references and a collection of known formulas and theorems on u_n, v_n . His application to binomial congruences is given under that topic.

G. Candido⁷⁷ gave the necessary and sufficient conditions, involving the u_k , that a polynomial x has the factor $x^2 - Px + Q$, whose roots are a, b .

A. Laparewicz⁷⁸ treated the factoring of $2^m \pm 1$ by Lucas' method.³⁹

E. B. Escott^{78a} showed the connection between Pisano's series and the puzzle to convert a square into a rectangle with one more (or fewer) units of area than the square.

E. B. Escott⁷⁹ applied Lucas' theory to the case $u_n = 2u_{n-1} + u_{n-2}$.

L. E. Dickson^{79a} proved that if z_k is the sum of the k th powers of the roots of $a^m + p_1 a^{m-1} + \dots + p_m = 0$, where the p 's are integers and $p_1 = 0$, then, in the series defined by $z_{x+m} + p_1 z_{x+m-1} + \dots + p_m z_x = 0$, z_t is divisible by t if t is a prime.

E. Landau⁸⁰ proved theorems on the divisors of U_m, V_m , where

$$(x+i)^m = U_m(x) + iV_m(x), \quad i = \sqrt{-1}.$$

P. Bachmann⁸¹ treated at length recurring series.

C. Ruggieri⁸² used Pisano's series for u_{-n} to solve for ξ and η

$$a\xi^2 + b\xi\eta + c\eta^2 = k, \quad b^2 - 4ac = 5m^2.$$

E. Zeuthen⁸³ proposed a problem on the series of Pisano.

H. Mathieu⁸⁴ noted that in $1, 3, 8, \dots, x_{n+1} = 3x_n - x_{n-1}$, the expressions $x_n x_{n+1} + 1, x_{n-1} x_{n+1} + 1$ are squares.

Valroff⁸⁵ stated in imperfect form theorems of Lucas.

A. Aubry⁸⁶ gave a summary of results by Genocchi¹⁵ and Lucas.

⁷²Mathesis, (3), 2, 1902, 60-62.

⁷³Periodico di Mat., 17, 1902, 320-5; l'intermédiaire des math., 23, 1916, 175-6.

⁷⁴L'intermédiaire des math., 10, 1903, 288.

⁷⁵Giornale di Mat., 42, 1904, 186-196.

⁷⁶Rendiconto Ac. Sc. Fis. e Mat. Napoli, (3), 10, 1904, 135-150.

⁷⁷Periodico di Mat., 20, 1905, 281-285.

⁷⁸Wiadomosci Matematyczne, Warsaw, 11, 1907, 247-256 (Polish).

^{78a}The Open Court, August, 1907. Reproduced by W. F. White, A Scrap-Book of Elementary Mathematics, Notes, Recreations, Essays, The Open Court Co., Chicago, 1908, 109-113.

⁷⁹L'intermédiaire des math., 15, 1908, 248-9.

^{79a}Amer. Math. Monthly, 15, 1908, 209.

⁸⁰Handbuch... Verteilung der Primzahlen, I, 1909, 442-5.

⁸¹Niedere Zahlentheorie, II, 1910, 55-96, 124.

⁸²Periodico di Mat., 25, 1910, 266-276.

⁸³Nyt Tidsskr. for Math., Kjobenhavn, A 22, 1911, 1-9. Solution by Fransen and Damm.

⁸⁴L'intermédiaire des math., 18, 1911, 222; 19, 1912, 87-90; 23, 1916, 14 (generalizations).

⁸⁵Ibid., 19, 1912, 145, 212, 285.

⁸⁶L'enseignement math., 15, 1913, 217-224

R. Niewiadomski⁸⁷ noted that, for a series of Pisano,

$$U_{N \pm a}^Z \equiv U_{\pm a+1}^Z \quad \text{or} \quad -U_{\pm a-1}^Z \pmod{N},$$

according as the prime $N = 10m \pm 1$ or $10m \pm 3$. He showed how to compute rapidly distant terms of the series of Pisano and similar series, and factored numerous terms.

L. Bastien⁸⁸ employed a prime p and integer $a_1 < p$ and determined a_2, a_3, \dots , each $< p$, by means of $a_1 a_2 \equiv Q$, $a_2 + a_3 \equiv P$, $a_3 a_4 \equiv Q$, $a_4 + a_5 \equiv P$, $\dots \pmod{p}$. Then

$$a_{2h+1} \equiv \frac{K_{h+1} a_1 - Q K_h}{K_h a_1 - Q K_{h-1}} \pmod{p}, \quad K_{h+1} = P K_h - Q K_{h-1}.$$

The types of series are found and enumerated. Every divisor of K_p is of the form $\lambda p \pm 1$. Some of Lucas' results are given.

R. D. Carmichael⁸⁹ generalized many of Lucas'^{38, 39} theorems and corrected several. The following is a generalization (p. 46) of Fermat's theorem: If $\alpha + \beta$ and $\alpha\beta$ are integers and $\alpha\beta$ is prime to $n = p_1^{a_1} \dots p_k^{a_k}$, where p_1, \dots, p_k are distinct primes, $u_\lambda = (\alpha^\lambda - \beta^\lambda)/(\alpha - \beta)$ is divisible by n when λ is the l. c. m. of

$$(3) \quad p_i^{a_i-1} \{p_i - (\alpha, \beta)_{p_i}\} \quad (i=1, \dots, k).$$

Here, if p is an odd prime, the symbol $(\alpha, \beta)_p$ denotes 0, +1 or -1, according as $(\alpha - \beta)^2$ is divisible by p , is a quadratic residue of p , or is a quadratic non-residue of p ; while $(\alpha, \beta)_2$ denotes +1 if $\alpha\beta$ is even, 0 if $\alpha\beta$ is odd and $\alpha + \beta$ is even, and -1 if $\alpha\beta(\alpha + \beta)$ is odd. In particular, if ϕ is the product of the numbers (3), $u_\phi \equiv 0 \pmod{n}$, which is the corrected form of the theorem of Lucas'²⁷.

Relations have been noted⁹⁰ between terms of recurring series defined by one of the equations

$$u_n + u_{n+1} = u_{n+2}, \quad u_n + u_{n+2} = u_{n+3}, \quad v_{n+1} + v_{n-1} = 4v_n, \quad v_1 = 1, \quad v_2 = 3.$$

E. Malo⁹¹ and Prompt⁹² considered the residues with respect to a prime modulus $10m \pm 1$ of the series $u_0, u_1, u_2 = u_0 + u_1, \dots, u_n = u_{n-1} + u_{n-2}$.

A. Boutin⁹³ noted relations between terms of Pisano's series.

A. Agronomof⁹⁴ treated $u_n = u_{n-1} + u_{n-2} + u_{n-3}$.

Boutin⁹⁵ and Malo⁹⁵ treated sums of terms of Pisano's series.

A. Pellet⁹⁶ generalized Lucas'²⁸ law of apparition of primes.

A. Gérardin⁹⁷ proved theorems on the divisors of terms of Pisano's series.

⁸⁷L'intermédiaire des math., 20, 1913, 51, 53-6.

⁸⁸Sphinx-Oedipe, 7, 1912, 33-38, 145-155.

⁸⁹Annals of Math., (2), 15, 1913, 30-70.

⁹⁰Math. Quest. Educat. Times, 23, 1913, 55; 25, 1914, 89-91.

⁹¹L'intermédiaire des math., 21, 1914, 86-8.

⁹²Ibid., 22, 1915, 31-6.

⁹³Mathesis, (4), 4, 1914, 126.

⁹⁴L'intermédiaire des math., 23, 1916, 64-7

⁹⁵Mathesis, (4), 4, 1914, 125.

⁹⁶L'intermédiaire des math., 23, 1916, 42-3.

⁹⁷Nouv. Ann. Math., (4), 16, 1916, 361-7.

E. Piccioli⁹⁸ noted that in Pisano's series 1, 1, 2, 3, . . . ,

$$u_k = \binom{k}{0} + \binom{k-1}{1} + \binom{k-2}{2} + \dots + t, \quad t = \left(\frac{1}{2}(k+1) \right) \text{ or } \left(\frac{1}{2}k \right),$$

according as k is odd or even.

T. A. Pierce⁹⁹ proved for the two functions $\Pi_{i=1}^n (1 \pm a_i^m)$ of the roots a_i of an equation with integral coefficients properties analogous to those of Lucas' u_n, v_n .

ALGEBRAIC THEORY OF RECURRING SERIES.

J. D. Cassini¹⁰⁰ and A. de Moivre¹⁰¹ treated series whose general term is a sum of a given number of preceding terms each multiplied by a constant. D. Bernoulli¹⁰² used such recurring series to solve algebraic equations. J. Stirling¹⁰³ permitted variable multipliers.

L. Euler¹⁰⁴ studied ordinary recurring series and their application to solving equations.

J. L. Lagrange¹⁰⁵ made the subject depend on the integration of linear equations in finite differences, treating also recurring series with an additive term. The general term of such a series was found by V. Riccati.¹⁰⁶

P. S. Laplace¹⁰⁷ made systematic use of generating functions and applied recurring series to questions on probability.

J. L. Lagrange¹⁰⁸ noted that if $Ay_k + By_{k+1} + \dots + Ny_{k+n} = 0$ is the recurring relation and if $A + Bt + \dots + Nt^n = 0$ has distinct roots α, β, \dots , the general term of the series is $y_x = \alpha\alpha^x + \beta\beta^x + \dots$. For the case of multiple roots he stated a formula which G. F. Malfatti¹⁰⁹ proved to be erroneous; the latter gave a new process explained for 2, 3 or 4 equal roots.

Lagrange¹¹⁰ had noticed independently his error and now gave the general term of a recurring series in the case of multiple roots by a more direct process than that of Malfatti.

Pietro Paoli¹¹¹ investigated the sum of a recurring series.

⁹⁸Periodico di Mat., 31, 1916, 284-7.

⁹⁹Annals of Math., (2), 18, 1916, 53-64.

¹⁰⁰Histoire acad. roy. sc. Paris, année 1680, 309.

¹⁰¹Phil. Trans. London, 32, 1722, 176; Miscellanea analytica, 1730, 27, 107-8; Doctrine of chances, ed. 2, 1738, 220-9.

¹⁰²Comm. Acad. Petrop., 3, ad annum 1728, 85-100.

¹⁰³Methodus differentialis, London, 1730, 1764.

¹⁰⁴Introductio in analysin infinitorum, 1748, I, Chs. 4, 13, 17. Cf. C. F. Degen, Det K. Danske Vidensk. Selskabs Aftand., 1, 1824, 135; Oversigt . . . Forhand., 1818-9, 4.

¹⁰⁵Miscellanea Taurinensia, 1, 1759, Math., 33-42; Oeuvres, I, 23-36.

¹⁰⁶Mém. présentés div. sav. Paris, 5, 1768, 153-174; Comm. Bonon., 5, 1767. Cf. M. Cantor, Geschichte Math., IV, 1908, 261.

¹⁰⁷Mém. sav. étr. ac. sc. Paris, 6, année 1771, 1774, p. 353; 7, année 1773, 1776; Oeuvres, VIII, 5-24, 69-197. Mém. ac. roy. sc. Paris, année, 1779, 1782, 207; Oeuvres, X, 1-89 (année 1777, 99).

¹⁰⁸Nouv. Mém. Ac. Berlin, année 1775, 1777, 183-272; Oeuvres, IV, 151.

¹⁰⁹Mem. mat. fis. soc. Ital., 3, 1786-7, 571.

¹¹⁰Nouv. Mém. Ac. Sc. Berlin, années 1792-3, 247; Oeuvres, V, 625-641 (p. 639 on the error).

¹¹¹Mem. Acad. Mantova, 1, 1795, 121. See Partitions in Vol. III of this History.

J. B. Fourier's^{111a} error in applying recurring series to the solution of numerical equations was pointed out by R. Murphy.^{111b}

P. Frisiani^{111c} applied recurring series to the solution of equations.

E. Betti^{111d} employed doubly recurring series to solve equations in two unknowns, by extending the method of Bernoulli.¹⁰²

W. Scheibner¹¹² considered a series with a three-term recursion formula, deduced the linear relation between any three terms, not necessarily consecutive, and applied his results to continued fractions and Gauss' hypergeometric series.

D. André¹¹³ deduced the generating equation of a recurring series V_i from that of a recurring series U_i , given a linear homogeneous relation between the terms V_i multiplied by constants and the terms U_n, U_{n-1}, \dots , multiplied by polynomials in n .

D. André¹¹⁴ considered a series U_1, U_2, \dots , with

$$U_n = u_n + \sum_{k=1}^{\lambda_n} A_k^{(n)} U_{n-k},$$

where u_n, λ_n are given functions of n , λ_n being an integer $\leq n-1$, while $A_k^{(n)}$ is a given function of k, n . It is proved that

$$U_n = \sum_{p=1}^n \Psi(n, p) u_p, \quad \Psi(n, p) = \sum A_{k_1}^{(n_1)} A_{k_2}^{(n_2)} \dots,$$

where the second summation extends over all sets of integral solutions of

$$k_1 + k_2 + \dots = n - p, \quad n_1 = k_1 + p, \quad n_i = k_i + n_{i-1} \quad (0 < k_i < \lambda_{n_i}).$$

Application is made to eight special types of series.

D. André¹¹⁵ discussed the sums of the series whose general terms are

$$\frac{u_n x^n}{n(n+1) \dots (n+p-1)}, \quad \frac{u_n x^{an+\beta}}{(an+\beta)!},$$

where u_n is the general term of any recurring series.

G. de Longchamps^{115a} proved the first result by Lagrange¹⁰⁸ and expressed y_x as a symmetric function of the distinct roots α, β, \dots . He^{115b} reduced $U_n = A_1 U_{n-1} + \dots + A_p U_{n-p} + f(n)$, where f is a polynomial of degree p , to the case $f(n) \equiv 0$ by making a substitution $U_n = V_n + \lambda_0 n^p + \dots + \lambda_p$.

C. A. Laisant^{115c} studied the ratios of consecutive terms of recurring series, in particular for Pisano's series.

^{111a}Analyse des équations, Paris, 1831.

^{111b}Phil. Mag., (3), 11, 1837, 38-40.

^{111c}Effemeridi Astronomiche di Milano, 1850, 3.

^{111d}Annali di Sc. Mat. Fis., 8, 1857, 48-61.

¹¹²Berichte Gesell. Wiss. Leipzig (Math.), 16, 1864, 44-68.

¹¹³Bull. Soc. Math. France, 6, 1877-8, 166-170.

¹¹⁴Ann. sc. l'école norm. sup., (2), 7, 1878, 375-408; 9, 1880, 209-226. Summary in Bull. des Sc. Math., (2), 1, I, 1877, 350-5.

¹¹⁵Comptes Rendus Paris, 86, 1878, 1017-9; 87, 1878, 973-5.

^{115a}Assoc. franç., 9, 1880, 91-6.

^{115b}Ibid., 1885, II, 94-100.

^{115c}Bull. des Sc. Math., (2), 5, I, 1881, 218-249.

M. d'Ocagne¹¹⁶ considered the recurring series U_i with

$$U_n = a_1 U_{n-1} + a_2 U_{n-2} + \dots + a_p U_{n-p},$$

and with U_0, \dots, U_{p-1} arbitrary; and the series u with the same law, but with $u_i = 0$ ($i = 0, \dots, p-2$), $u_{p-1} = 1$. Then

$$U_n = U_0 u_{n+p-1} + (U_1 - a_1 U_0) u_{n+p-2} + \dots + (U_{p-1} - a_1 U_{p-2} - \dots - a_{p-1} U_0) u_n.$$

For each series he found the sum of any fixed number of consecutive terms and the limit of that sum.

M. d'Ocagne¹¹⁷ treated $u_{p+n} = u_{p+n-1} + \dots + u_n$. He¹¹⁸ discussed the convergents to a periodic continued fraction by use of $u_n = a_n u_{n-1} + (-1)^n u_{n-2}$, $u_0 = 0$, $u_1 = 1$.

L. Gegenbauer^{118a} found the solution P_m of $g_n P_n = 2^\lambda u_n P_{n-1} + \psi_n P_{n-2}$, where

$$P_0 = 1, \quad P_1 = 2^\lambda, \quad g_n = 2^{\kappa n a} u_{1n}, \quad \psi_n = 2^{2\lambda + \sigma + a \sigma n} u_{2n}.$$

S. Pincherle^{118b} applied $p_{n+1}(x) = (x - \alpha_n)(x - \beta_n)p_n(x)$ to developments in series.

E. Study^{118c} showed how to express the general term of a recurring series as a sum of the general terms of simpler recurring series, exhibited explicitly the general term when $n = 3$, and applied the theory to bilinear forms.

M. d'Ocagne¹¹⁹ considered a recurring series with the law of recurrence

$$(A_1, \dots, A_p): \quad Y_n + A_1 Y_{n-1} + \dots + A_p Y_{n-p} = 0$$

of order p and generating equation

$$\Phi(x) = x^p + A_1 x^{p-1} + \dots + A_p = 0.$$

Set

$$Q_i(x) = x^i + A_1 x^{i-1} + \dots + A_i, \quad \Psi(x) = Y_{p-1} + Q_1(x) Y_{p-2} + \dots + Q_{p-1}(x) Y_0.$$

The existence of a common root α of $\Phi(x) = 0$, $\Psi(x) = 0$ is a necessary and sufficient condition that the Y 's satisfy also a law of recurrence of order $p-1$, viz., $(Q_1(\alpha), \dots, Q_{p-1}(\alpha))$, and then the initial law of recurrence is said to be reducible to one of order $p-1$.

M. d'Ocagne¹²⁰ considered the series with the law of recurrence

$$u_n^i = a_{i0}^i u_{n-1}^i + a_{i1}^i u_{n-2}^i + \dots + a_{ip-1}^i u_{n-p}^i$$

and generating equation

$$\phi_i(x) = x^{p_i} - a_{i0}^i x^{p_i-1} - \dots - a_{ip-1}^i,$$

¹¹⁶Nouv. Ann. Math., (3), 2, 1883, 220-6; 3, 1884, 65-90; 9, 1890, 93-7; 11, 1892, 526-532 (5, 1886, 257-272). Bull. Soc. Math. France, 12, 1883-4, 78-90 (case $p=2$); 15, 1886-7, 143-4; 19, 1890-1, 37-9 (minor applications). Nieuw Archief voor Wiskunde, 17, 1890, 229-232 (applications to $\sin ma$ as function of $\sin a$ and $\cos a$).

¹¹⁷Comptes Rendus Paris, 104, 1887, 419-420; errata, 534.

¹¹⁸Ibid., 108, 1889, 499-501.

^{118a}Sitzungsber Ak. Wiss. Wien (Math.), 97, IIa, 1888, 82-89.

^{118b}Atti R. Accad. Lincei, Rendiconti, 5, 1889, I, 8-12, 323-7.

^{118c}Monatshefte Math. Phys., 2, 1891, 22-54.

¹¹⁹Bull. Soc. Math. France, 20, 1892, 121-2.

¹²⁰Comptes Rendus Paris, 115, 1892, 790-2; errata, 904.

such that, for $i=0$, $u_0 = \dots = u_{p-2} = 0$, $u_{p-1} = 1$. If $\phi_0(x) = \phi_1(x) \cdots \phi_m(x)$,

$$u_{n+p-1}^{(0)} = \sum u_{n_1+p_1-1}^1 \cdots u_{n_m+p_m-1}^m,$$

summed for all combinations of n 's for which $n_1 + \dots + n_m = n$. Application is made to the sum of a recurring series with a variable law of recurrence.

M. d'Ocagne¹²¹ reproduced the last result, and gave a connected exposition of his earlier results and new ones.

R. Perrin¹²² considered a recurring series U of order p with the terms u_0, u_1, \dots . The general term of the k th derived series of U is defined to be

$$u_n^{(k)} = \begin{vmatrix} u_n & u_{n+1} & \dots & u_{n+k} \\ u_{n+1} & u_{n+2} & \dots & u_{n+k+1} \\ \dots & \dots & \dots & \dots \\ u_{n+k} & u_{n+k+1} & \dots & u_{n+2k} \end{vmatrix}.$$

If any term of the $(p-1)$ th derived series is zero, the law of recurrence of the given series U is reducible (to one of lower order). If also any term of the $(p-2)$ th derived series is zero, continue until we get a non-vanishing determinant; then its order is the minimum order of U . This criterion is only a more convenient form of that of d'Ocagne.^{119, 121}

E. Maillet¹²³ noted that a necessary condition that a law of recurrence of order p be reducible to one of order $p-q$ is that $\Phi(x)$ and $\Psi(x)$ of d'Ocagne¹¹⁹ have q roots in common, the condition being also sufficient if $\Phi(x)=0$ has only distinct roots. He found independently a criterion analogous to that of Perrin¹²² and studied series with two laws of recurrence.

J. Neuberg¹²⁴ considered $u_n = au_{n-1} + bu_{n-2}$ and found the general term of the series of Pisano.

C. A. Laisant¹²⁵ treated the case F a constant of d'Ocagne's¹²¹ $u_k \{f(u)\} = F(k)$.

S. Lattès¹²⁶ treated $u_{n+p} = f(u_{n+p-1}, \dots, u_n)$, where f is an analytic function.

M. Amsler¹²⁷ discussed recurring series by partial fractions.

E. Netto,^{127a} L. E. Dickson,^{127b} A. Ranum,¹²⁸ and T. Hayashi¹²⁹ gave the general term of a recurring series. N. Traverso¹³⁰ gave the general term for $Q_n = (n-1)(Q_{n-1} + Q_{n-2})$ and $u_n = au_{n-1} + bu_{n-2}$.

Traverso¹³¹ applied the theory of combinations with repetitions to express, as a function of p , the solution of $Q_m = p(Q_{m-1} + Q_{m-2} + \dots + Q_{m-n})$.

¹²¹Jour. de l'école polyt., 64, 1894, 151-224.

¹²²Comptes Rendus Paris, 119, 1894, 990-3.

¹²³Mém. Acad. Sc. Toulouse, (9), 7, 1895, 179-180, 182-190; Assoc. franç., 1895, III, 233 [report with miscellaneous Dioph. equations of order n , Vol. II]; Nouv. Ann. Math., (3), 14, 1895, 152-7, 197-206.

¹²⁴Mathesis, (2), 6, 1896, 88-92; Archivo de mat., 1, 1896, 230.

¹²⁵Bull. Soc. Math. France, 29, 1901, 145-9.

¹²⁶Comptes Rendus Paris, 150, 1910, 1106-9.

¹²⁷Nouv. Ann. Math., (4), 10, 1910, 90-5.

^{127a}Monatshefte Math. Phys., 6, 1895, 285-290.

^{127b}Amer. Math. Monthly, 10, 1903, 223-6.

¹²⁸Bull. Amer. Math. Soc., 17, 1911, 457-461.

¹²⁹Ibid., 18, 1912, 191-2.

¹³⁰Periodico di Mat., 29, 1913-4, 101-4; 145-160.

¹³¹Ibid., 31, 1915-6, 1-23, 49-70, 97-120, 145-163, 193-207.

F. Nicita¹³² found many relations like $2a_n^2 - b_n^2 = -(-1)^n$ between the two series $a_1=1, a_2=2, \dots, a_n=\frac{1}{2}(a_{n+1}-a_{n-1}), \dots; b_1=1, b_2=3, \dots, b_n=\frac{1}{2}(b_{n+1}-b_{n-1}), \dots$

Reference may be made to the text by A. Vogt¹³³ and to texts and papers on difference equations cited in *Encyklopädie der Math. Wiss.*, I, 2, pp. 918, 935; *Encyclopédie des Sc. Math.*, I, 4, 47-85.

A. Weiss¹³⁴ expressed the general term t_k of a recurring series of order r linearly in terms of $t_q, t_{q-1}, \dots, t_{q-r+1}$, where q is an integer.

W. A. Whitworth¹³⁵ proved that, if $c_0+c_1x+c_2x^2+\dots$ is a convergent recurring series of order r whose first $2r$ terms are given, its scale of relation and sum to infinity are the quotients of certain determinants.

H. F. Scherk¹³⁶ started with any triangle ABC and on its sides constructed outwards squares $BCED, ACFG, ABJH$. Join the end points to form the hexagon $DEFGHJ$. Then construct squares on the three joining lines EF, GH, JD and again join the end points to form a new hexagon, etc. If a_i, b_i, c_i are the lengths of the joining lines in the i th set, $a_{n+1}=5a_{n-1}-a_{n-3}$. The n th term is found as usual.

Sylvester¹³⁷ solved $u_x = u_{x-1} + (x-1)(x-2)u_{x-2}$. A. Tarn¹³⁸ treated recurring series connected with the approximations to $\sqrt{2}, \sqrt{3}, \sqrt{5}$.

V. Schlegel¹³⁹ called the development of $(1-x-x^2-\dots-x^n)^{-1}$ the $(n-1)$ th series of Lamé; each coefficient is the sum of the n preceding. For $n=2$, the series is that of Pisano.

References on the connection between Pisano's series and leaf arrangement and golden section (Kepler, Braun, etc.) have been collected by R. C. Archibald.¹⁴⁰

Papers by C. F. Degen,¹⁴¹ A. F. Svanberg,¹⁴² and J. A. Vész¹⁴³ were not available for report.

¹³²*Periodico di Mat.*, 32, 1917, 200-210, 226-36.

¹³³*Theorie der Zahlenreihen u. der Reihengleichung*, Leipzig, 1911, 133 pp.

¹³⁴*Jour. für Math.*, 38, 1849, 148-157.

¹³⁵Oxford, Cambridge and Dublin *Mess. Math.*, 3, 1866, 117-121; *Math. Quest. Educ. Times*, 3, 1865, 100-1.

¹³⁶*Abh. Naturw. Vereine zu Bremen*, 1, 1868, 225-236.

¹³⁷*Math. Quest. Educ. Times*, 13, 1870, 50.

¹³⁸*Math. Quest. and Solutions*, 1, 1916, 8-12.

¹³⁹*El Progreso Mat.*, 4, 1894, 171-4.

¹⁴⁰*Amer. Math. Monthly*, 25, 1918, 232-8.

¹⁴¹*Mém. Acad. Sc. St. Pétersbourg*, 1821-2, 71.

¹⁴²*Nova Acta R. Soc. Sc. Upsaliensis*, 11, 1839, 1.

¹⁴³*Értekez. a Math., Magyar Tudom. Ak. (Math. Memoirs Hungarian Ac. Sc.)*, 3, 1875, No. 1.

CHAPTER XVIII.

THEORY OF PRIME NUMBERS.

EXISTENCE OF AN INFINITUDE OF PRIMES.

Euclid¹ noted that, if p were the greatest prime, and $M = 2 \cdot 3 \cdot 5 \dots p$ is the product of all the primes $\leq p$, then $M+1$ is not divisible by one of those primes and hence has a prime factor $> p$, thus involving a contradiction.

L. Euler² deduced the theorem from the [invalid] equation

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod \left(1 - \frac{1}{p}\right)^{-1},$$

the left member being infinite and the right finite if there be only a finite number of primes. Euler³ concluded from the same equation that "the number of primes exceeds the number of squares."

Euler⁴ modified Euclid's¹ argument slightly. The number of integers $< M$ and prime to M is $\phi(M) = 2 \cdot 4 \dots (p-1)$, so that they include integers which are either primes $> p$ or have prime factors $> p$.

The theorem follows from Tchebychef's²⁶¹ proof of Bertrand's postulate.

L. Kronecker⁵ noted that we may rectify Euler's² proof by using

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \left(1 - \frac{1}{p^s}\right)^{-1} \quad (s > 1),$$

where p ranges over all primes > 1 . If there were only a finite number of p 's, the product would remain finite when s approaches unity, while the sum increases indefinitely. He also gave the proof a form leading to an interval from m to n within which there exists a new prime however great m is taken.

R. Jaensch⁶ repeated Euler's² argument, also ignoring convergency.

E. Kummer⁷ gave essentially Euler's⁴ argument.

J. Perott⁸ noted that, if p_1, \dots, p_n are the primes $\leq N$, there are 2^n integers $\leq N$ which are not divisible by a square, and

$$2^n > N - \sum_{k=1}^n \left[\frac{N}{p_k^2} \right] > N \left(1 - \sum \frac{1}{p_k^2}\right) > N \left(2 - \frac{\pi^2}{6}\right) > \frac{N}{3}.$$

Hence there exist infinitely many primes.

L. Gegenbauer^{8a} proved the theorem by means of $\sum_{n=1}^{\infty} n^{-s}$.

¹Elementa, IX, 20; Opera (ed., Heiberg), 2, 1884, 388-91.

²Introductio in analysin infinitorum, 1, Ch. 15, Lausanne, 1748, p. 235; French transl. by J. B. Labey, 1, 218.

³Comm. Acad. Petrop., 9, 1737, 172-4.

⁴Posthumous paper, Comm. Arith. Coll., 2, 518, Nos. 134-6; Opera Postuma, I, 1862, 18.

⁵Vorlesungen über Zahlentheorie, I, 1901, 269-273, Lectures of 1875-6.

⁶Die Schwierigeren Probl. Zahlentheorie, Progr. Rastenburg, 1876, 2.

⁷Monatsber. Ak. Wiss. Berlin für 1878, 1879, 777-8.

⁸Bull. sc. math. et astr., (2), 5, 1881, I, 183-4.

^{8a}Sitzungsber. Ak. Wiss. Wien (Math.), 95, II, 1887, 94-6; 97, IIa, 1888, 374-7.

J. Perott⁹ applied the theory of commutative groups to show that, if q_1, \dots, q_n are primes, there exist at least $n-1$ primes between q_n and $M = q_1 \cdots q_n$.

T. J. Stieltjes¹⁰ expressed the product P of the primes $2, 3, \dots, p$ as a product AB of two factors in any way. Since $A+B$ is not divisible by $2, \dots, p$, there exists a prime $> p$.

J. Hacks¹¹ proved the existence of an infinitude of primes by use of his formula (Ch. XI, Hacks¹⁴) for the number of integers $\leq m$ not divisible by a square.

C. O. Boije af Gennäs¹² showed how to find a prime exceeding the n th prime $p_n > 2$. Take $P = 2^{v_1} 3^{v_2} \cdots p_n^{v_n}$, each $v_i \geq 1$. Express P as a product of relatively prime factors $\delta, P/\delta$, where $Q = P/\delta - \delta > 1$. Since Q is divisible by no prime $\leq p_n$, it is a product of powers of primes $q_i \geq p_n + 2$. Take δ so that $Q < (p_n + 2)^2$. Then Q is a prime.

Axel Thue¹³ proved that, if $(1+n)^k < 2^n$, there exist at least $k+1$ primes $< 2^n$.

J. Braun^{13a} noted that the sum of the inverses of the primes $\leq p$ is, for $p \geq 5$, an irreducible fraction > 1 ; hence the numerator contains at least one prime $> p$. He attributed to Hacks a proof by means of $\Pi(1 - 1/p^2)^{-1} = \Sigma s^{-2} = \pi^2/6$; the product would be rational if there were only a finite number of primes, whereas π is irrational.

E. Cahen¹⁴ proved the "identity of Euler" used by Kronecker.⁵

Störmer²⁸⁸ gave a proof.

A. Lévy¹⁵ took a product P of k of the first n primes p_1, \dots, p_n and the product Q of the remaining $n-k$. Then $P+Q$ is either prime or has a prime factor $> p_n$; likewise for $P-Q$. If p_n is a prime such that p_n+2 is composite, there exist at least n primes $> p_n$, but $\leq 1 + p_1 p_2 \cdots p_n$. When

$$\pm \frac{1}{p_1} \pm \dots \pm \frac{1}{p_n}$$

is reduced to a simple fraction, the numerator has no factor in common with $p_1 \cdots p_n$; hence there is a prime $> p_n$. He considered (pp. 242-4) the primes defined by $x(x-1)-1$ for consecutive integers x .

A. Auric¹⁶ assumed that p_1, \dots, p_k give all the primes. Then the number of integers $< n = \Pi p_i^{a_i}$ is

$$< \Pi(a_i + 1) < \left(\frac{\log np_k}{\log p_1} \right)^k,$$

which is small in comparison with n , whence k increases indefinitely with n .

⁹Amer. Jour. Math., 11, 1888, 99-138; 13, 1891, 235-308, especially 303-5.

¹⁰Annales fac. sc. de Toulouse, 4, 1890, 14, final paper.

¹¹Acta Math., 14, 1890-1, 335.

¹²Öfversigt K. Sv. Vetenskaps-Akad. Förhand., Stockholm, 50, 1893, 469-471.

¹³Archiv for Math. og Natur., Kristiania, 19, 1897, No. 4, 1-5.

^{13a}Das Fortschrittsgesetz der Primzahlen durch eine transcendente Gleichung exakt dargestellt, Wiss. Beilage Jahresbericht, Gymn., Trier, 1899, 96 pp.

¹⁴Éléments de la théorie des nombres, 1900, 319-322.

¹⁵Bull. de Math. Élémentaires, 15, 1909-10, 33-34, 80-82.

¹⁶L'intermédiaire des math., 22, 1915, 252.

G. Métrod¹⁷ noted that the sum of the products $n-1$ at a time of the first n primes > 1 is either a prime or is divisible by a prime greater than the n th. He also repeated Euler's⁴ proof.

INFINITUDE OF PRIMES IN A GENERAL ARITHMETICAL PROGRESSION.

L. Euler²⁰ stated that an arithmetical progression with the first term unity contains an infinitude of primes.

A. M. Legendre²¹ claimed a proof that there is an infinitude of primes $2mx + \mu$ if $2m$ and μ are relatively prime.

Legendre²² noted that the theorem would follow from the following lemma: Given any two relatively prime integers A, C , and any set of k odd primes $\theta, \lambda, \dots, \omega$ [not divisors of A], and denoting the z th odd prime by $\pi^{(z)}$, then among $\pi^{(k-1)}$ consecutive terms of the progression $A - C, 2A - C, 3A - C, \dots$ there occurs at least one divisible by no one of the primes θ, \dots, ω . Although Legendre supposed he had proved this lemma, it is false [Dupré²³].

G. L. Dirichlet²³ gave the first proof that $mz + n$ represents infinitely many primes if m and n are relatively prime. The difficult point in the proof is the fact that

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0,$$

where $\chi(n) = 0$ if n, k have a common factor > 1 , while, in the contrary case, $\chi(n)$ is a real character different from the chief character of the group of the classes of residues prime to k modulo k . This point Dirichlet proved by use of the classes of binary quadratic forms.

Dirichlet²⁴ extended the theorem to complex integers.

E. Heine²⁵ proved "without higher calculus" Dirichlet's result

$$\lim_{\rho=0} \rho \left\{ \frac{1}{(b+a)^{1+\rho}} + \frac{1}{(b+2a)^{1+\rho}} + \dots \right\} = \frac{1}{a}.$$

A. Desboves²⁶ discussed the error in Legendre's²² proof.

L. Durand²⁷ gave a false proof.

A. Dupré²⁸ showed that the lemma of Legendre²² is false and gave (p. 61) the following theorem to replace it: The mean number of terms,

¹⁷L'intermédiaire des math., 24, 1917, 39-40.

²⁰Opusc. analytica, 2, 1785 (1775), 241; Comm. Arith., 2, 116-126.

²¹Mém. ac. sc. Paris, année 1785, 1788, 552.

²²Théorie des nombres, ed. 2, 1808, p. 404; ed. 3, 1830, II, p. 76; Maser, 2, p. 77.

²³Bericht Ak. Wiss. Berlin, 1837, 108-110; Abhand. Ak. Wiss. Berlin, Jahrgang 1837, 1839, Math., 45-71; Werke, 1, 1889, 307-12, 313-42. French transl., Jour. de Math., 4, 1839, 393-422. Jour. für Math., 19, 1839, 368-9; Werke, 1, 460-1. Zahlentheorie, §132, 1863; ed. 2, 1871; 3, 1879; 4, 1894 (p. 625, for a simplification by Dedekind).

²⁴Abhand. Ak. Wiss. Berlin, Jahrgang 1841, 1843, Math., 141-161; Werke, 1, 509-532. French transl., Jour. de Math., 9, 1844, 245-269.

²⁵Jour. für Math., 31, 1846, 133-5.

²⁶Nouv. Ann. Math., 14, 1855, 281.

²⁷Ibid., 1856, 296.

²⁸Examen d'une proposition de Legendre, Paris, 1859. Comptes Rendus Paris, 48, 1859, 487.

prime to $\theta, \lambda, \dots, \omega$, contained in $\pi^{(k-1)}$ consecutive terms of the progression is $\geq P^{-1}Q\pi^{(k-1)} - 2$, where $P = 3 \cdot 5 \cdot 7 \cdot 11 \dots$, $Q = (3-1)(5-1) \dots$.

J. J. Sylvester²⁹ gave a proof.

V. I. Berton^{29a} found h such that between x and xh occur at least $2g$ primes each of one of the $2g$ linear forms $2py + r_i$, where r_1, \dots, r_{2g} are the integers $< 2p$ and prime to $2p$.

C. Moreau³⁰ noted the error in Legendre's²² proof.

L. Kronecker⁵ (pp. 442-92) gave in lectures, 1886-7, the following extension* of Dirichlet's theorem (in lectures, 1875-6, for the case m a prime): If μ is any given integer, we can find a greater integer ν such that, if m, r are any two relatively prime integers, there exists at least one prime of the form $hm + r$ in the interval from μ to ν (p. 11, pp. 465-6). Moreover (pp. 478-9), there is the same mean density of primes in each of the $\phi(m)$ progressions $mh + r_i$, where the r_i are the integers $< m$ and prime to m .

I. Zignago³¹ gave an elementary proof.

H. Scheffler³² devoted 31 pages to a revision of Legendre's insufficient proof and gave a process to determine all primes under a given limit.

G. Speckmann³³ failed in an attempt to prove the theorem.

P. Bachmann³⁴ gave an exposition of Dirichlet's²³ proof.

Ch. de la Vallée-Poussin³⁵ obtained without computations, by use of the theory of functions of a complex variable, a proof of the difficult point in Dirichlet's²³ proof. He³⁶ proved that the sum of the logarithms of the primes $hk + l \leq x$ equals $x/\phi(k)$ asymptotically and concluded readily that the number of primes $hk + l \leq x$ equals, asymptotically,

$$\frac{1}{\phi(k)} \cdot \frac{x}{\log x}.$$

F. Mertens³⁷ proved the existence of an infinitude of primes in an arithmetical progression by elementary methods not using the quadratic reciprocity theorem or the number of classes of primitive binary quadratic forms. He supplemented the theorem by showing how to find a constant c such that between x and cx there lies at least one prime of the progression for every $x \geq 1$ [cf. Kronecker,⁵ pp. 480-96].

²⁹Proc. London Math. Soc., 4, 1871, 7; Messenger Math., (2), 1, 1872, 143-4; Coll. Math. Papers, 2, 1908, 712-3.

^{29a}Comptes Rendus Paris, 74, 1872, 1390.

³⁰Nouv. Ann. Math., (2), 12, 1873, 323-4. Also, A. Piltz, Diss., Jena, 1884.

*Improvements in the exposition were made by the editor, Hensel (cf. p. 508).

³¹Annali di Mat., (2), 21, 1893, 47-55.

³²Beleuchtung u. Beweis eines Satzes aus Legendre's Zahlentheorie [II, 1830, 76], Leipzig, 1893.

³³Archiv Math. Phys., (2), 12, 1894, 439-441. Cf. (2), 15, 1897, 326-8.

³⁴Die analytische Zahlentheorie, 1894, 51, 74-88.

³⁵Mém. couronnés... acad. roy. sc. Belgique, 53, 1895-6, No. 6, 24-9.

³⁶Annales de la soc. sc. de Bruxelles, 20, 1896, II, 281-361. Cf. 183-256, 361-397; 21, 1897, I, 1-13, 60-72; II, 251-368.

³⁷Sitzungsber. Ak. Wiss. Wien (Math.), 106, 1897, IIa, 254-286. Parts published earlier, *ibid.*, 104, 1895, IIa, 1093-1121, 1158-1166; Jour. für Math., 78, 1874, 46-62; 117, 1897, 169-184.

F. Mertens³⁸ gave a proof, still simpler than his³⁷ earlier one, of the difficult point in Dirichlet's²³ proof. The proof is very elementary, involving computations of finite sums.

F. Mertens³⁹ gave a simplification of Dirichlet's²⁴ proof of his generalization to complex primes.

H. Teege⁴⁰ proved the difficult point in Dirichlet's²³ proof.

E. Landau⁴¹ proved that the number of prime ideals of norm $\leq x$ of an algebraic field equals the integral-logarithm $Li(x)$ asymptotically. By specialization to the fields defined by $\sqrt{-1}$ or $\sqrt{-3}$, we derive theorems⁴² on the number of primes $4k \pm 1$ or $6k \pm 1 \leq x$.

L. E. Dickson⁴³ asked if $a_i n + b_i$ ($i = 1, \dots, m$) represent an infinitude of sets of m primes, noting necessary conditions.

H. Weber⁴⁴ proved Dirichlet's²⁴ theorem on complex primes.

E. Landau⁴⁵ simplified the proofs by de la Vallée-Poussin³⁵ and Mertens.³⁸

E. Landau^{46, 47} simplified Dirichlet's²³ proof. Landau⁴⁸ proved that, if k, l are relatively prime, the number of primes $ky + l \leq x$ is

$$\frac{1}{\phi(k)} \int_2^x \frac{du}{\log u} + O(xe^t), \quad t \equiv -\sqrt[3]{\log x},$$

where γ is a constant depending on k . For O see Pfeiffer⁹⁰ of Ch. X.

A. Cunningham⁴⁹ noted that, of the N primes $\leq R$, approximately $N/\phi(n)$ occur in the progressions $nx + a$, $a < n$ and prime to n , and gave a table showing the degree of approximation when $R = 10^5$ or $5 \cdot 10^5$, with n even and < 1928 . Within these limits there are fewer primes $nx + 1$ than primes $nx + a$, $a > 1$.

INFINITUDE OF PRIMES REPRESENTED BY A QUADRATIC FORM.

G. L. Dirichlet⁵⁵ gave in sketch a proof that every properly primitive quadratic form (a, b, c) , $a, 2b, c$ with no common factor, represents an infinitude of primes.

Dirichlet⁵⁶ announced the extension that among the primes represented by (a, b, c) , an infinitude are representable by any given linear form $Mx + N$, with M, N relatively prime, provided a, b, c, M, N are such that the linear and quadratic forms can represent the same number.

³⁸Sitzungsber. Ak. Wiss. Wien (Math.), 108, 1899, IIa, 32-37.

³⁹*Ibid.*, 517-556. Polish transl. in *Prace mat. fiz.*, 11, 1900, 194-222.

⁴⁰Mitt. Math. Gesell. Hamburg, 4, 1901, 1-11.

⁴¹Math. Annalen, 56, 1903, 665-670.

⁴²Sitzungsber. Ak. Wiss. Wien (Math.), 112, 1903, IIa, 502-6.

⁴³Messenger Math., 33, 1904, 155.

⁴⁴Jour. für Math., 129, 1905, 35-62. Cf. p. 48.

⁴⁵Sitzungsber. Akad. Berlin, 1906, 314-320.

⁴⁶Rend. Circ. Mat. Palermo, 26, 1908, 297.

⁴⁷Handbuch ... Verteilung der Primzahlen, I, 1909, 422-35.

⁴⁸Sitzungsber. Ak. Wiss. Wien (Math.), 117, 1908, IIa, 1095-1107.

⁴⁹Proc. London Math. Soc., (2), 10, 1911, 249-253.

⁵⁵Bericht Ak. Wiss. Berlin, 1840, 49-52; Werke, 1, 497-502. Extract in Jour. für Math., 21, 1840, 98-100.

⁵⁶Comptes Rendus Paris, 10, 1840, 285-8; Jour. de Math., 5, 1840, 72-4; Werke, 1, 619-623.

H. Weber⁵⁷ and E. Schering⁵⁸ completed Dirichlet's⁵⁵ proof of his first theorem. A. Meyer⁵⁹ completed Dirichlet's⁵⁶ proof of his extended theorem.

F. Mertens⁶⁰ gave an elementary proof of Dirichlet's⁵⁵ extended theorem.

Ch. de la Vallée-Poussin³⁶ proved that the number of primes $\leq x$ representable by a properly primitive definite positive or indefinite⁶¹ irreducible binary quadratic form is asymptotic to $gx/\log x$, where g is a constant; and the same for primes belonging also to a linear form compatible with the character of the quadratic form.

L. Kronecker⁵ (pp. 494-5) stated a theorem on factorable forms in several variables which represent an infinitude of primes.

ELEMENTARY PROOFS OF THE EXISTENCE OF AN INFINITUDE OF PRIMES $mz+1$,
FOR ANY GIVEN m .

V. A. Lebesgue⁶⁵ gave a proof for the case m a prime, using the fact that $x^{m-1} - x^{m-2}y + \dots + y^{m-1}$ has besides the possible factor m only prime factors $2km+1$. A like method applies^{65a} to $2mz-1$.

J. A. Serret⁶⁶ gave an incomplete proof for any m .

F. Landry⁶⁷ gave a proof like Lebesgue's.⁶⁵ If θ is the largest prime $2km+1$ and if x is the product of all of them, x^m+1 is divisible by no one of them. Since $(x^m+1)/(x+1)$ has no prime divisor not of the form $2km+1$, there exists at least one $>\theta$.

A. Genocchi⁶⁸ proved the existence of an infinitude of primes $mz\pm 1$ and $n^iz\pm 1$ for n a prime by use of the rational and irrational parts of $(a+\sqrt{b})^k$.

L. Kronecker⁵ (pp. 440-2) gave in lectures, 1875-6, a proof for the case m a prime; the simple extension in the text to any m was added by Hensel.

E. Lucas gave a proof by use of his u_n (Lucas,³⁹ p. 291, of Ch. XVII).

A. Lefébure³⁰ of Ch. XVI stated that the theorem follows from his results.

L. Kraus⁶⁹ gave a proof.

A. S. Bang⁷⁰ and Sylvester⁸³ proved it by use of cyclotomic functions.

K. Zsigmondy⁷⁸ of Ch. VII gave a proof. Also, E. Wendt,⁷¹ and Birkhoff and Vandiver⁶² of Ch. XVI.

⁵⁷Math. Annalen, 20, 1882, 301-329. Elliptische Functionen (=Algebra, III), ed. 2, 1908, 613-6.

⁵⁸Werke, 2, 1909, 357-365, 431-2.

⁵⁹Jour. für Math., 103, 1888, 98-117. Exposition by Bachmann,³⁴ pp. 272-307.

⁶⁰Sitzungsber. Ak. Wiss. Wien (Math.), 104, 1895, IIa, 1093-1153, 1158. Simplification, *ibid.*, 109, 1900, IIa, 415-480.

⁶¹Cf. E. Landau, Jahresber. D. Math. Verein., 24, 1915, 250-278.

⁶²Jour. de Math., 8, 1843, 51, note. Exercices d'analyse numérique, 1859, 91.

⁶³Jour. de Math., (2), 7, 1862, 417.

⁶⁴Jour. de Math., 17, 1852, 186-9.

⁶⁵Deuxième mémoire sur la théorie des nombres, Paris, 1853, 3.

⁶⁶Annali di mat., (2), 2, 1868-9, 256-7. Cf. Genocchi²², ⁶¹ of Ch. XVII.

⁶⁷Casopis Math. a Fys., 15, 1886, 61-2. Cf. Fortschritte, 1886, 134-5.

⁷⁰Tidsskrift for Math., (5), 4, 1886, 70-80, 130-7. See Bang²³, ²⁴, Ch. XVI.

⁷¹Jour. für Math., 115, 1895, 85.

N. V. Bervi⁷² proved that the ratio of the number of integers $cm+1$ not $>n$ and not a product of two integers of that form to the number of all primes not $>n$ has the limit unity for $n = \infty$.

H. C. Pocklington⁷³ proved that, if n is any integer, there is an infinitude of primes $mn+1$, an infinitude not of this form if $n > 2$, and an infinitude not of the forms $mn \pm 1$ if $n = 5$ or $n > 6$.

E. Cahen⁷⁴ proved the theorem for m an odd prime.

J. G. van der Corput⁷⁵ proved the theorem.

ELEMENTARY PROOFS OF THE EXISTENCE OF AN INFINITUDE OF PRIMES IN
SPECIAL ARITHMETICAL PROGRESSIONS.

J. A. Serret⁶⁶ for the common difference 8 or 12, and for $10x+9$.

V. A. Lebesgue⁸⁰ for $4n \pm 1$, $8n+k$ ($k=1, 3, 5, 7$). Lebesgue⁸¹ for the same and $2^m n+1$, $6n-1$. Also, by use of infinite series, for the common difference 8 or 12.

E. Lucas⁸² for $5n+2$, $8n+7$.

J. J. Sylvester⁸³ for the difference 8 or 12 and⁸⁴ for $p^k x-1$, p a prime.

A. S. Bang⁸⁵ for the differences 4, 6, 8, 10, 12, 14, 18, 20, 24, 30, 42, 60.

E. Lucas⁸⁶ for $4n \pm 1$, $6n-1$, $8n+5$.

R. D. von Sterneck⁸⁷ for $an-1$.

K. Th. Vahlen⁸⁸ for $mz+1$ by use of Gauss' periods of roots of unity. Also, if m is any integer and p a prime such that $p-1$ is divisible by a higher power of 2 than $\phi(m)$ is, while k is a root of $km+1 \equiv -1 \pmod{p}$, the linear form $mpx+km+1$ represents an infinitude of primes; known special cases are $mx+1$ and $2px-1$.

J. J. Iwanow⁸⁹ for the difference 8 or 12.

E. Cahen¹⁴ (pp. 318-9) for $4x \pm 1$, $6x \pm 1$, $8x+5$. K. Hensel⁵ (pp. 438-9, 508) for the same forms. M. Bauer⁹⁰ for $an-1$.

E. Landau⁴⁷ (pp. 436-46) for $kn \pm 1$.

I. Schur⁹¹ proved that if $l^2 \equiv 1 \pmod{k}$ and if one knows a prime $> \phi(k)/2$ of the form $kz+l$, there exists an infinitude of primes $kz+l$; for example,

$$2^nz+2^{n-1} \pm 1, \quad 8mz+2m+1, \quad 8mz+4m+1, \quad 8mz+6m+1,$$

where m is any odd number not divisible by a square.

K. Hensel⁹² for $4n \pm 1$, $6n \pm 1$, $8n-1$, $8n \pm 3$, $12n-1$, $10n-1$.

⁷²Mat. Sbornik (Math. Soc. Moscow), 18, 1896, 519.

⁷³Proc. Cambr. Phil. Soc., 16, 1911, 9-10. ⁷⁴Nouv. Ann. Math., (4), 11, 1911, 70-2.

⁷⁵Nieuw Archief voor Wiskunde, (2), 10, 1913, 357-361 (Dutch).

⁸⁰Nouv. Ann. Math., 15, 1856, 130, 236.

⁸¹Exercices d'analyse numérique, 1859, 91-5, 103-4, 145-6.

⁸²Amer. Jour. Math., 1, 1878, 309.

⁸³Comptes Rendus Paris, 106, 1888, 1278-81, 1385-6.

⁸⁴Assoc. franç. av. sc., 17, 1888, II, 118-120.

⁸⁵Nyt Tidsskrift for Math., Kjobenhavn, 1891, 2B, 73-82.

⁸⁶Théorie des nombres, 1891, 353-4.

⁸⁷Monatshefte Math. Phys., 7, 1896, 46.

⁸⁸Schriften phys.-ökon. Gesell. Königsberg, 38, 1897, 47.

⁸⁹Math. Soc. St. Petersburg, 1899, 53-8 (Russian).

⁹⁰Jour. für Math., 131, 1906, 265-7; transl. of Math. és Phys. Lapok, 14, 1905, 313.

⁹¹Sitzungsber. Berlin Math. Gesell., 11, 1912, 40-50, with Archiv M. P.

⁹²Zahlentheorie, 1913, 304-5.

R. D. Carmichael⁹³ for $p^k n - 1$ (p an odd prime) and $2^k \cdot 3n - 1$.

M. Bauer's⁹⁴ paper was not available for report.

POLYNOMIALS REPRESENTING NUMEROUS PRIMES.

Chr. Goldbach¹⁰⁰ noted that a polynomial $f(x)$ cannot represent primes exclusively, since the constant term would be unity, whereas it is $f(p)$ in $f(x+p)$.

L. Euler¹⁰¹ proved this by noting that, if $f(a) = A$, $f(nA+a)$ is divisible by A .

Euler¹⁰² noted that $x^2 - x + 41$ is a prime for $x = 1, \dots, 40$.

Euler¹⁰³ noted that $x^2 + x + 17$ is a prime for $x = 0, 1, \dots, 15$ and [error] 16; $x^2 + x + 41$ is a prime for $x = 0, 1, \dots, 15$.

A. M. Legendre¹⁰⁴ noted that $x^2 + x + 41$ is a prime for $x = 0, 1, \dots, 39$, that $2x^2 + 29$ is a prime for $x = 0, 1, \dots, 28$, and gave a method of finding such functions. [Replacing x by $x+1$ in Euler's¹⁰² function, we get $x^2 + x + 41$.] If $\beta^2 + 2(a+\beta)x - 13x^2$ is a square only when $x=0$, and a and β are relatively prime, then $a^2 + 2a\beta + 14\beta^2$ is a prime or double a prime. He gave many such results.

Chabert^{104a} stated that $3n^2 + 3n + 1$ represents many primes for n small.

G. Oltramare¹⁰⁵ noted that $x^2 + ax + b$ has no prime divisor $\leq \mu$ and hence is a prime when $< \mu^2$, if $a^2 - 4b$ is a quadratic non-residue of each of the primes $2, 3, \dots, \mu$. The function $x^2 + ax + (a^2 + 163)/4$ is suitable to represent a series of primes. Taking $x=0$, $a=u/v$, he stated that $u^2 + 163v^2$ or its quotient by 4 gives more than 100 primes between 40 and 1763.

H. LeLasseur¹⁰⁶ verified that, for a prime A between 41 and 54000, $x^2 + x + A$ does not represent primes exclusively for $x = 0, 1, \dots, A-2$.

E. B. Escott¹⁰⁷ noted that $x^2 + x + 41$ gives primes not only for $x = 0, 1, \dots, 39$, but also¹⁰⁸ for $x = -1, -2, \dots, -40$. Hence, replacing x by $x-40$, we get $x^2 - 79x + 1601$, a prime for $x = 0, 1, \dots, 79$. Several such functions are given.

Escott¹⁰⁹ examined values of A much exceeding 54000 in $x^2 + x + A$ without finding a suitable $A > 41$. Legendre's¹⁰⁴ first seven formulas for primes give composite numbers for $a=2$, the eighth for $a=3$, etc. Escott found that $x^3 + x^2 + 17$ is a prime for $x = -14, -13, \dots, +10$. In $x^3 - x^2 - 17$ replace x by $x-10$; we get a cubic which is a prime for $x = 0, 1, \dots, 24$.

⁹³Annals of Math., (2), 15, 1913, 63-5.

⁹⁴Archiv Math. Phys., (3), 25, 1916, 131-4.

¹⁰⁰Corresp. Math. Phys. (ed., Fuss), I, 1843, 595, letter to Euler, Nov. 18, 1752.

¹⁰¹Novi Comm. Acad. Petrop., 9, 1762-3, 99; Comm. Arith., 1, 357.

¹⁰²Mém. de Berlin, année 1772, 36; Comm. Arith., 1, 584.

¹⁰³Opera postuma, I, 1862, 185. In Pascal's Repertorium Höheren Math., German transl. by Schepp, 1900, I, 518, it is stated incorrectly to be a prime for the first 17 values of x ; likewise by Legendre, Théorie des nombres, 1798, 10; 1808, 11.

¹⁰⁴Théorie des nombres, 1798, 10, 304-312; ed. 2, 1808, 11, 279-285; ed. 3, 1830, I, 248-255; German transl. by Maser, I, 322-9.

^{104a}Nouv. Ann. Math., 3, 1844, 250.

¹⁰⁶Mém. l'Inst. Nat. Genevois, 5, 1857, No. 2, 7 pp.

¹⁰⁶Nouv. Corresp. Math., 5, 1879, 371; quoted in l'intermédiaire des math., 5, 1898, 114-5.

¹⁰⁷L'intermédiaire des math., 6, 1899, 10-11.

¹⁰⁸The same 40 primes as for $x = 0, \dots, 39$, as noted by G. Lemaire, *ibid.*, 16, 1909, p. 197.

¹⁰⁹*Ibid.*, 17, 1910, 271.

E. Miot¹¹⁰ stated that $x^2 - 2999x + 2248541$ is a prime for $1460 \leq x \leq 1539$.

G. Frobenius¹¹¹ proved that the value of $x^2 + xy + py^2$ is a prime if $< p^2$, that of $2x^2 + py^2$ (y odd) if $< p(2p+1)$, that of $x^2 + 2py^2$ (x odd) if $< p(p+2)$, and noted cases in which an indefinite form $x^2 + xy - qy^2$ is a prime.

Lévy¹⁵ examined $x^2 - x - 1$. He¹¹² considered $f(x) = ax^2 + abx + c$, where a, b, c are integers, $0 \leq a < 4$. Giving to x the values $0, 1, 2, \dots$, we get a set of integers such that, for every n exceeding a certain value, $f(n)$ is either prime or admits a prime factor which divides a number $f(p)$, where $p < n$. For example, if for $f(x) = x^2 - x + 41$ we grant that $f(0), f(1), f(2), f(3)$ and $f(4)$ are primes, we can conclude that $f(x)$ is prime for $x \leq 40$. Likewise when 41 is replaced by 11 or 17. Again, $2x^2 - 2x + 19$ and $3x^2 - 3x + 23$ give successions of 18 and 22 primes respectively. Bouniakowsky³⁵ of Ch. XI considered polynomials which represent an infinitude of primes.

Braun^{13a} proved that there exists no quotient of two polynomials such that the greatest integer contained in its numerical value is a prime for all integral values $> k$ of the variable.

GOLDBACH'S EMPIRICAL THEOREM: EVERY EVEN INTEGER IS A SUM OF TWO PRIMES.

Chr. Goldbach¹²⁰ conjectured that every number N which is a sum of two primes is a sum of as many primes including unity as one wishes (up to N), and that every number > 2 is a sum of three primes.

L. Euler¹²¹ remarked that the first conjecture can be confirmed from an observation previously communicated to him by Goldbach that every even number is a sum of two primes. Euler expressed his belief in the last statement, though he could not prove it. From it would follow that, if n is even, $n, n-2, n-4, \dots$ are the sums of two primes and hence n a sum of 3, 4, 5, \dots primes.

R. Descartes¹²² stated that every even number is a sum of 1, 2 or 3 primes.

E. Waring¹²³ stated Goldbach's theorem and added that every odd number is either a prime or is a sum of three primes.

L. Euler¹²⁴ stated without proof that every number of the form $4n+2$ is a sum of two primes each of the form $4k+1$, and verified this for $4n+2 \leq 110$.

¹¹⁰L'intermédiaire des math., 19, 1912, 36. [From $X^2 + X + 41$ by setting $X = x - 1500$.]

¹¹¹Sitz. Ak. Wiss. Berlin, 1912, 966-980.

¹¹²Bull. Soc. Math. France, 1911, Comptes Rendus des Séances. Extract in Sphinx-Oedipe, 9, 1914, 6-7.

¹²⁰Corresp. Math. Phys. (ed., P. H. Fuss), 1, 1843, p. 127 and footnote; letter to Euler, June 7, 1742.

¹²¹Ibid., p. 135; letter to Goldbach, June 30, 1742. Cited by G. Eneström, Bull. Bibl. Storia Sc. Mat. e Fis., 18, 1885, 468.

¹²²Posthumous manuscript, Oeuvres, 10, 298.

¹²³Meditationes Algebraicae, 1770, 217; ed. 3, 1782, 379. The theorem was ascribed to Waring by O. Terquem, Nouv. Ann. Math., 18, 1859, Bull. Bibl. Hist., p. 2; by E. Catalan, Bull. Bibl. Storia Sc. Mat. e Fis., 18, 1885, 467; and by Lucas, Théorie des Nombres, 1891, 353.

¹²⁴Acta Acad. Petrop., 4, II, 1780 (1775), 38; Comm. Arith. Coll., 2, 1849, 135.

A. Desboves¹²⁵ verified that every even number between 2 and 10000 is a sum of two primes in at least two ways; while, if the even number is the double of an odd number, it is simultaneously a sum of two primes of the form $4n+1$ and also a sum of two primes of the form $4n-1$.

J. J. Sylvester¹²⁶ stated that the number of ways of expressing a very large even number n as a sum of two primes is approximately the ratio of the square of the number of primes $< n$ to n , and hence bears a finite ratio to the quotient of n by the square of the natural logarithm of n . [Cf. Stäckel¹³²].

F. J. E. Lionnet¹²⁷ designated by x the number of ways $2a$ can be expressed as a sum of two odd primes, by y the number of ways $2a$ can be expressed as a sum of two distinct odd composite numbers, by z the number of odd primes $< 2a$, and by q the largest integer $\leq a/2$. He proved that $q+x=y+z$ and argued that it is very probable that there are values of n for which $q=y+z$, whence $x=0$.

N. V. Bougaief^{127a} noted that, if $M(n)$ denotes the number of ways n can be expressed as a sum of two primes, and if θ_i denotes the i th prime > 1 ,

$$\sum_i (n - 3\theta_i) M(n - \theta_i) = 0.$$

G. Cantor¹²⁸ verified Goldbach's theorem up to 1000. His table gives the number of decompositions of each even number < 1000 as a sum of two primes and lists the smaller prime.

V. Aubry¹²⁹ verified the theorem from 1002 to 2000.

R. Haussner¹³⁰ verified the law up to 10000 and announced results observed by a study of his¹³¹ tables up to 5000. His table I (pp. 25-178) gives the number ν of decompositions of every even n up to 3000 as a sum $x+y$ of two primes and the values of x ($x \leq y$), as in the table by Cantor. His table II (pp. 181-191) gives ν for $2 < n < 5000$; this table and further computations enable him to state that Goldbach's theorem is true for $n < 10000$. Let $P(2\rho+1)$ be the number of all odd primes 1, 3, 5, . . . which are $\leq 2\rho+1$, and set

$$\xi(2\rho+1) = P(2\rho+1) - 2P(2\rho-1) + P(2\rho-3), \quad P(-1) = P(-3) = 0.$$

Then the number of decompositions of $2n$ into a sum of two primes x, y ($x \leq y$) is

$$\sum_{\rho=0}^{n-1} P(2n-2\rho-1) \xi(2\rho+1).$$

If $\epsilon = 1$ or -1 according as n is a prime or not,

$$\nu = \frac{1}{2} \sum_{\rho=1}^{n-1} P(2n-2\rho-1) \xi(2\rho+1) + \frac{\epsilon}{2}.$$

¹²⁵Nouv. Ann. Math., 14, 1855, 293.

¹²⁶Proc. London Math. Soc., 4, 1871-3, 4-6; Coll. M. Papers, 2, 709-711.

¹²⁷Nouv. Ann. Math., (2), 18, 1879, 356. Cf. Assoc. franç. av. sc., 1894, I, p. 96.

^{127a}Comptes Rendus Paris, 100, 1885, 1124.

¹²⁸Assoc. franç. av. sc., 1894, 117-134; l'intermédiaire des math., 2, 1895, 179.

¹²⁹L'intermédiaire des math., 3, 1896, 75; 4, 1897, 60; 10, 1903, 61 (errata, p. 166, p. 283).

¹³⁰Jahresbericht Deutschen Math.-Verein., 5, 1896, 62-66. Verhandlungen Gesell. Deutscher Naturforscher u. Aerzte, 1896, II, 8.

¹³¹Nova Acta Acad. Caes. Leop.-Carolinae, 72, 1899, 1-214.

Table III gives the values of P and ξ for each odd number $2\rho+1 < 5000$.

P. Stäckel¹³² noted that Lionnet's¹²⁷ argument is not conclusive, and designated by G_{2n} the number of all decompositions of $2n$ as a sum of two primes (counting $p+q$ and $q+p$ as two different decompositions). If P_k is the number of all odd primes from 1 to k ,

$$\sum_{n=1}^{\infty} G_{2n} x^{2n} = (\sum x^p)^2 = (1-x^2)^2 \left(\sum_{p=0}^{\infty} P_{2p+1} x^{2p+1} \right)^2,$$

where p ranges over all the odd primes. Approximations to G_{2n} for n large in terms of Euler's ϕ -function are

$$\frac{P_{2n}^2}{\phi(2n)}, \quad \frac{[P(2n - \sqrt{2n}) - P(\sqrt{2n})]^2}{n - \sqrt{2n}} \cdot \frac{n}{\phi(2n)},$$

where $P(k)$ is written for P_k for convenience in printing. Lack of agreement with Sylvester¹²⁶ is noted; cf. Landau.¹³⁵ It is stated that the truth of Goldbach's theorem is made very probable [but not proved¹³³].

Sylvester^{133a} stated that any even integer $2n$ is a sum of two primes, one $> n/2$ and the other $< 3n/2$, whence it is possible to find two primes whose difference is less than any given number and whose sum is twice that number.

F. J. Studnicka¹³⁴ discussed Sylvester's statement.

Sylvester^{134a} stated that, if N is even and λ, \dots, ω are the θ primes $> \frac{1}{4}N$ and $< \frac{3}{4}N$ (excluding $\frac{1}{2}N$ if it be prime), the number of ways of composing N [by addition] with two of these primes is the coefficient of x^N in

$$\left(\frac{1}{1-x^\lambda} + \dots + \frac{1}{1-x^\omega} \right)^r / r(r-1)\theta^{-2} \quad (r \geq 2).$$

E. Landau¹³⁵ noted that Stäckel's approximation to G_n is

$$\mathfrak{G}_n = \frac{n^2}{\log^2 n \phi(n)},$$

and showed that $\sum_{n=1}^x G_n$ has the true approximation $\frac{1}{2}x^2/\log^2 x$. By a longer analysis, he proved that if we use Stäckel's \mathfrak{G}_n to form the sum, we do not obtain a result of the correct order of magnitude.

L. Ripert¹³⁶ examined certain large even numbers.

E. Mœillet¹³⁷ proved that every even number ≤ 350000 (or 10^6 or $9 \cdot 10^6$) is, in default by at most 6 (or 8 or 14), the sum of two primes.

A. Cunningham¹³⁸ verified Goldbach's theorem for all numbers up to 200 million which are of the forms

$$(4 \cdot 3)^n, \quad (4 \cdot 5)^n, \quad 2 \cdot 10^n, \quad 2^n (2^n \mp 1), \quad a \cdot 2^n, \quad 2a^n, \quad (2a)^n, \quad 2(2^n \mp a),$$

for $a = 1, 3, 5, 7, 9, 11$. He reduced the formula of Haussner for ν to a form more convenient for computation.

¹³²Göttingen Nachrichten, 1896, 292-9.

^{133a}Nature, 55, 1896-7, 196, 269.

^{134a}Educ. Times, Jan. 1897. Proof by J. Hammond, Math. Quest. Educ. Times, 26, 1914, 100.

¹³⁵Göttingen Nachrichten, 1900, 177-186.

¹³⁶L'intermédiaire des math., 10, 1903, 67, 74, 166 (errors, p. 168).

¹³⁷Ibid., 12, 1905, 107-9.

¹³³Encyclopédie des sc. math., I, 17, p. 339, top.

¹³⁴Casopis, Prag, 26, 1897, 207-8.

¹³⁸Messenger Math., 36, 1906, 17-30.

J. Merlin¹³⁹ considered the operation $A(b, a)$ of effacing from the natural series of integers all the numbers $ax+b$. The effect of carrying out one of the two sets of operations $A(r_1, p_1)$, $A(r_i, p_i)$, $A(r'_i, p_i)$, $i=2, \dots, n$, where p_n is the n th prime >1 , is equivalent to constructing a crib of Eratosthenes up to p_n . It is stated that in every interval of length $\nu p_n \log p_n$ there is at least one number not effaced, if ν is independent of n . It is said to follow that, for a sufficiently large, there exist two primes having the sum $2a$. Under specified assumptions, there exist an infinitude of n 's for which $p_{n+1} - p_n = 2$.

M. Vecchi¹⁴⁰ wrote p_n for the n th odd prime and called p_h and p_{h+a} of the same order if $p_h^2 > p_{h+a}$. Then $2n > 132$ is a sum of two primes of the same order in $[\frac{1}{2}(\phi+1)]$ ways if and only if there exist ϕ numbers not $> n - p_{m+1} + 1$ and not representable in any of the forms

$$a_i + 3x, \quad b_i + 5x, \dots, \quad l_i + p_m x \quad (i=1, 2),$$

where p_{m+1} is the least prime p for which $p^2 + p > 2n$, and the known terms a_i, \dots are the residues with respect to the odd prime occurring as coefficient of x .

*G. Giovannelli, Sul teorema di Goldbach, Atri, 1913.

THEOREMS ANALOGOUS TO GOLDBACH'S.

Chr. Goldbach¹⁴⁵ stated empirically that every odd number is of the form $p + 2a^2$, where p is a prime and a is an integer ≥ 0 . L. Euler¹⁴⁶ verified this up to 2500. Euler¹²⁴ verified for $m = 8N + 3 \leq 187$ that m is the sum of an odd square and the double of a prime $4n + 1$.

J. L. Lagrange¹⁴⁷ announced the empirical theorem that every prime $4n - 1$ is a sum of a prime $4m + 1$ and the double of a prime $4h + 1$.

A. de Polignac¹⁴⁸ conjectured that every even number is the difference of two consecutive primes in an infinitude of ways. His verification up to 3 million that every odd number is the sum of a prime and a power of 2 was later^{148a} admitted to be in error for 959.

M. A. Stern¹⁴⁹ and his students found that $53 \cdot 109 = 5777$ and $13 \cdot 641 = 5993$ are neither of the form $p + 2a^2$ and verified that up to 9000 there are no further exceptions to Goldbach's¹⁴⁵ assertion. Also, 17, 137, 227, 977, 1187 and 1493 are the only primes < 9000 not of the form $p + 2b^2$, $b > 0$. Thus all odd numbers < 9000 , which are not of the form $6n + 5$, are of the form $p + 2b^2$.

E. Lemoine¹⁵⁰ stated empirically that every odd number > 3 is a sum of a prime p and the double of a prime π , and is also of the forms $p - 2\pi$ and $2\pi' - p'$.

¹³⁹Comptes Rendus Paris, 153, 1911, 516-8. Bull. des. sc. math., (2), 39, I, 1915, 121-136. In a prefatory note, J. Hadamard noted that, while the proof has a lacuna, it is suggestive.

¹⁴⁰Atti Reale Accad. Lincei, Rendiconti, (5), 22, II, 1913, 654-9.

¹⁴⁶Corresp. Math. Phys. (ed., Fuss), 1, 1843, 595; letter to Euler, Nov. 18, 1752.

¹⁴⁸Ibid., p. 596, 606; Dec. 16, 1752.

¹⁴⁷Nouv. Mém. Ac. Berlin, année 1775, 1777, 356; Oeuvres, 3, 795.

¹⁴⁸Nouv. Ann. Math., 8, 1849, 428 (14, 1855, 118).

^{148a}Comptes Rendus Paris, 29, 1849, 400, 738-9.

¹⁴⁹Nouv. Ann. Math., 15, 1856, 23.

¹⁵⁰L'intermédiaire des math., 1, 1894, 179; 3, 1896, 151.

H. Brocard¹⁵¹ gave an incorrect argument by use of Bertrand's postulate that there exists a prime between any two consecutive triangular numbers.

G. de Rocquigny¹⁵² remarked that it seems true that every multiple of 6 is the difference of two primes of the form $6n+1$.

Brocard¹⁵³ verified this property for a wide range of values.

L. Kronecker¹⁵⁴ remarked that an unnamed writer¹⁴⁸ had stated empirically that every even number can be expressed in an infinitude of ways as the difference of two primes. Taking 2 as the number, we conclude that there exist an infinitude of pairs of primes differing by 2.

L. Ripert¹⁵⁵ verified that every even number < 10000 is a sum of a prime and a power, every odd one except 1549 is such a sum.

E. Maillet¹⁵⁶ commented on de Polignac's conjecture that every even number is the difference of two primes.

E. Maillet¹⁵⁷ proved that every odd number < 60000 (or $9 \cdot 10^6$) is, in default by at most 8 (or 14), the sum of a prime and the double of a prime.

PRIMES IN ARITHMETICAL PROGRESSION.

E. Waring¹⁶⁵ stated that if three primes (the first of which is not 3) are in arithmetical progression, the common difference d is divisible by 6, except for the series 1, 2, 3 and 1, 3, 5. For 5 primes, the first of which is not 5, d is divisible by 30; for 7 primes, the first not 7, d is divisible by $2 \cdot 3 \cdot 5 \cdot 7$; for 11 primes, the first not 11, d is divisible by $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$; and similarly for any prime number of primes in arithmetical progression, a property easily proved. Hence by continually adding d to a prime, we reach a number divisible by 3, 5, . . . , unless d is divisible by 3, 5, . . .

J. L. Lagrange¹⁶⁶ proved that if 3 primes, no one being 3, are in arithmetical progression, the difference d is divisible by 6; for 5 primes, no one being 5, d is divisible by 30. He stated that for 7 primes, d is divisible by $2 \cdot 3 \cdot 5 \cdot 7$, unless the first one is 7, and then there are not more than 7 consecutive prime terms in a progression whose difference is not divisible by $2 \cdot 3 \cdot 5 \cdot 7$.

E. Mathieu¹⁶⁷ proved Waring's statement.

M. Cantor¹⁶⁸ proved that if $P = 2 \cdot 3 \cdot \dots \cdot p$ is the product of all the primes up to the prime p , there is no arithmetical progression of p primes, no one of which is p , unless the common difference is divisible by P . He conjectured that three successive primes are not in arithmetical progression unless one of them is 3.

A. Guibert¹⁶⁹ gave a short proof of the theorem stated thus: Let p_1, \dots, p_n be primes ≥ 1 in arithmetical progression, where n is odd and > 3 . Then no prime > 1 and $\leq n$ is a p_i . If n is a prime and is a p_i , then $i = 1$.

¹⁵¹*L'intermédiaire des math.*, 4, 1897, 159. Criticism by E. Landau, 20, 1913, 153.

¹⁵²*Ibid.*, 5, 1898, 268.

¹⁵³*L'intermédiaire des math.*, 6, 1899, 144.

¹⁵⁴*Vorlesungen über Zahlentheorie*, 1, 1901, 68.

¹⁵⁵*L'intermédiaire des math.*, 10, 1903, 217-8.

¹⁵⁶*Ibid.*, 12, 1905, 108.

¹⁵⁷*Ibid.*, 13, 1906, 9.

¹⁵⁸*Meditationes Algebraicae*, 1770; ed. 3, 1782, 379.

¹⁶⁶*Nouv. Mém. Ac. Berlin*, année 1771, 1773, 134-7.

¹⁶⁷*Nouv. Ann. Math.*, 19, 1860, 384-5.

¹⁶⁸*Zeitschrift Math. Phys.*, 6, 1861, 340-3.

¹⁶⁹*Jour. de Math.*, (2), 7, 1862, 414-6.

The common difference is divisible by each prime $\leq n$, and by n itself if n is a prime not in the series.

H. Brocard^{169a} gave several sets of five consecutive odd integers, four of which are primes. Lionnet^{169b} had asked if the number of such sets is unlimited.

G. Lemaire¹⁷⁰ noted that $7+30n$ and $107+30n$ ($n=0, 1, \dots, 5$) are all primes; also $7+150n$ and $47+210n$ ($n=0, \dots, 6$).

E. B. Escott¹⁷¹ found conditions that $a+210n$ ($n=0, 1, \dots, 9$) be all primes and noted that the conditions are satisfied if $a=199$.

Devignot¹⁷² noted the primes $47+210n$, $71+2310n$ ($n=0, 1, \dots, 6$).

A. Martin¹⁷³ gave numerous sets of primes in arithmetical progression.

TESTS FOR PRIMALITY.

The fact that n is a prime if and only if it divides $1+(n-1)!$ was noted by Leibniz,⁷ Lagrange,¹⁸ Genty,²⁴ Lebesgue,⁸⁵ and Catalan,¹⁰⁶ cited in Chapter III, where was discussed the converse of Fermat's theorem in furnishing a primality test. Tests by Lucas, etc., were noted in Ch. XVII. Further tests have been noted under Cipolla¹⁷² and¹⁷⁶ Cole¹⁷³ of Ch. I, Sardi²⁷³ of Ch. III, Lambert⁶ of Ch. VI, Zsigmondy⁷⁹ of Ch. VII, Gegenbauer^{80, 92} of Ch. X, Jolivald⁸⁴ of Ch. XIII, Euler,²⁶⁻⁴³ Tchebychef,⁵² Schaffgotsch¹⁰⁰ and Biddle¹⁴¹ of Ch. XIV, Hurwitz⁴¹ and Cipolla⁴⁵ of Ch. XV. See also the papers by von Koch,²³⁵ Hayashi,^{239, 240} Andreoli,²⁴⁴ and Petrovitch²⁴⁵ of the next section.

L. Euler¹⁷⁷ gave a test for the primality of a number $N=4m+1$ which ends with 3 or 7. Let R be the remainder on subtracting from $2N$ the next smaller square $(5n)^2$ which ends with 5. To R add $100(n-1)$, $100(n-3)$, $100(n-5)$, If among R and these sums there occurs a single square, N is a prime or is divisible by this square. But if no square occurs or if two or more squares occur, N is composite. For example, if $N=637$, $(5n)^2=1225$, $R=49$; among 49, 649, 1049, 1249 occurs only the square 49; hence N is a prime or is divisible by 49 [$N=49 \cdot 13$].

W. L. Kraft¹⁷⁸ noted that $6m+1$ is a prime if m is of neither of the forms $6xy \pm (x+y)$; $6m-1$ is a prime if $m \neq 6xy+x-y$.

A. S. de Montferrier¹⁷⁹ noted that an odd number A is a prime if and only if $A+k^2$ is not a square for $k=1, 2, \dots, (A-3)/2$.

M. A. Stern¹⁸⁰ noted that n is a prime if and only if it occurs $n-1$ times in the $(n-1)$ th set, where the first set is 1, 2, 1; the second set, formed by inserting between any two terms of the first set their sum, is 1, 3, 2, 3, 1; etc.

^{169a}Nouv. Ann. Math., (3), 15, 1896, 389-90.

^{169b}Nouv. Ann. Math., (3), 1, 1882, 336.

¹⁷⁰L'intermédiaire des math., 16, 1909, 194-5.

¹⁷¹Ibid., 17, 1910, 285-6.

¹⁷²Ibid., 45-6.

¹⁷³School Science and Mathematics, 13, 1913, 793-7,

¹⁷⁶Doubt as to the sufficiency of Cole's test has been expressed, Proc. London Math. Soc., (2), 16, 1917-8.

¹⁷⁷Opera postuma, I, 188-9 (about 1778).

¹⁷⁸Nova Acta Acad. Petrop., 12, 1801, hist., p. 76, mem., p. 217.

¹⁷⁹Corresp. Math. Phys. (ed., Quetelet), 5, 1829, 94-6.

¹⁸⁰Jour. für Math., 55, 1858, 202.

L. Gegenbauer¹⁸¹ noted that $4n+1$ is a prime if

$$\left[\frac{4n+1-y^2}{4y} \right] = \left[\frac{4n-3-y^2}{4y} \right]$$

for every odd y , $1 < y \leq \sqrt{4n+1}$, and gave two similar tests for $4n+3$.

D. Gambioli¹⁸² and O. Meissner¹⁸³ discussed the impracticability of the test by the converse of Wilson's theorem.

J. Hacks¹⁸⁴ gave the characteristic relations for primes p :

$$\sum_{y=1}^{p-1} \sum_{s=1}^{p-1} \left[\frac{ys}{p} \right] = \left(\frac{p-1}{2} \right)^2 (p-2), \quad \sum_{y=1}^{p-1} \left\{ \sum_{s=1}^{(p-1)/2} \left[\frac{ys}{p} \right] + \sum_{s=1}^{\lfloor y/2 \rfloor} \left[\frac{ps}{y} \right] \right\} = \left(\frac{p-1}{2} \right)^3.$$

K. Zsigmondy¹⁸⁵ noted that a number is a prime if and only if not expressible in the form $\alpha_1 \alpha_2 + \beta_1 \beta_2$, where the α 's and β 's are positive integers such that $\alpha_1 + \alpha_2 = \beta_1 - \beta_2$. An odd number C is a prime if and only if $C+k^2$ is not a square for $k=0, 1, \dots, [(C-9)/6]$.

R. D. von Sterneck^{185a} gave several criteria for the $(s+1)$ th prime by use of partitions into elements formed from the first s primes.

H. Laurent^{185b} noted that

$$(e^{2\pi i \Gamma(z)/z} - 1) / (e^{-2\pi i/z} - 1)$$

equals 0 or 1 according as z is composite or prime.

Fontebasso¹⁸⁶ noted that N is a prime if not divisible by one of the primes $2, 3, \dots, p$, where $N/p < p+4$.

H. Laurent¹⁸⁷ proved that if we divide

$$F_n(x) = \prod_{j=1}^{n-1} (1-x^j)(1-x^{2j}) \dots (1-x^{(n-1)j})$$

by $(x^n-1)/(x-1)$, the remainder is 0 or x^{n-1} according as n is composite or prime. If we take x to be an imaginary root of $x^n=1$, $F_n(x)$ becomes 0 or x^{n-1} in the respective cases.

Helge von Koch¹⁸⁸ used infinite series to test whether or not a number is a power of a prime.

Ph. Jolivald¹⁸⁹ noted that, since every odd composite number is the difference of two triangular numbers, an odd number N is a prime if and only if there is no odd square, with a root $\leq (2N-9)/3$, which increased by $8N$ gives a square.

S. Minetola¹⁹⁰ noted that, if $k-n$ is divisible by $2n+1$, then $2k+1$ is composite. We may terminate the examination when we reach a prime $2n+1$ for which $(k-n)/(2n+1) \leq n$.

A. Bindoni¹⁹¹ added that we may stop with a prime giving $(k-n)$

¹⁸¹Sitzungsber. Ak. Wiss. Wien (Math.), 99, IIa, 1890, 389.

¹⁸²Periodico di Mat., 13, 1898, 208-212.

¹⁸⁴Acta Mathematica, 17, 1893, 205.

^{185a}Sitzungsber. Ak. Wiss. Wien (Math.), 105, IIa, 1896, 877-882.

^{185b}Comptes Rendus Paris, 126, 1898, 809-810.

¹⁸⁷Nouv. Ann. Math., (3), 18, 1899, 234-241.

¹⁸⁸Öfversigt Vetén.-Akad. Förhand., 57, 1900, 789-794 (French).

¹⁸⁹L'intermédiaire des math., 9, 1902, 96; 10, 1903, 20.

¹⁹⁰Il Boll. Matematica Giorn. Sc.-Didat., Bologna, 6, 1907, 100-4.

¹⁸³Math. Naturw. Blätter, 3, 1906, 100

¹⁸⁵Monatsh. Math. Phys., 5, 1894, 123-8.

¹⁸⁶Suppl. Periodico di Mat., 1899, 53.

¹⁹¹Ibid., 165-6.

$\div (2n+1) \leq n+2a-1$, where a is the difference between $2n+1$ and the next greater prime.

F. Stasi¹⁹² noted that N is a prime if not divisible by one of the primes $2, 3, \dots, p$, where $N/p < p+2a$ and a is the difference between p and the prime just $> p$.

E. Zondadari¹⁹³ noted that

$$\frac{\sin^2 \pi x}{(\pi x)^2 (1-x^2)^2} \prod_{n=2}^{\infty} \frac{\pi x}{n \sin \pi x/n}$$

is zero when $x = \pm p$ (p a prime) and not otherwise.

A. Chiari¹⁹⁴ cited known tests for primes, as the converse of Wilson's theorem.

H. C. Pocklington¹⁹⁵ employed single valued functions $\phi(x)$, $\psi(x)$, vanishing for all positive integers x (as $\phi = \psi = \sin \pi x$), and real, finite and not zero for all other positive values of x . Then, for the gamma function Γ ,

$$\phi^2(x) + \psi^2\left(\frac{1+\Gamma(x)}{x}\right)$$

is zero if and only if x is a prime [Wigert^{236a}].

E. B. Escott¹⁹⁶ stated that if we choose a_1, \dots, a_n, b so that the coefficients of $x^{2n}, x^{2n-2}, \dots, x^2$ in the expansion of

$$(x^n + a_1 x^{n-1} + \dots + a_n)^2 (x+b)$$

are all zero, then all the remaining coefficients, other than the first and last, are divisible by $2n+1$ if and only if $2n+1$ is a prime.

J. de Barinaga¹⁹⁷ concluded from Wilson's theorem that if $(P-1)!$ is divided by $1+2+\dots+(P-1) = P(P-1)/2$, the remainder is $P-1$ when P is a prime, but is zero when P is composite (not excluding $P=4$ as in the converse of Wilson's theorem). Hence on increasing by unity the least positive residues $\neq 0$ obtained on dividing $1 \cdot 2 \cdot \dots \cdot x$ by $1+2+\dots+x$, for $x = 1, 2, 3, \dots$, we obtain the successive odd primes $3, 5, \dots$

M. Vecchi¹⁴⁰ noted that, if $x \geq 1$, $N > 2$ is a prime if and only if it be of the form $2^x \pi' - \pi$, where π is the product of all odd primes $\leq p$, p being the largest odd prime $\leq [\sqrt{N}]$, and where π' is a product of powers of primes $> p$ with exponents ≥ 0 . Again, $N > 121$ is a prime if and only if of the form $\pi - 2^y \pi'$ where $y \geq 1$.

Vecchi¹⁹⁸ gave the simpler test: $N > 5$ is a prime if and only if $\alpha - \beta = N$, $\alpha + \beta = \pi$, for α, β relatively prime, where π is the product of all the odd primes $\leq [\sqrt{N}]$.

G. Rados¹⁹⁹ noted that p is a prime if and only if $\{2!3! \dots (p-2)!(p-1)!\}^4 \equiv 1 \pmod{p}$.

Carmichael⁹³ gave several tests analogous to those by Lucas.

¹⁹²Il Boll. Matematica Giorn. Sc.-Didat., Bologna, 6, 1907, 120-1.

¹⁹³Rend. Accad. Lincei, (5), 19, 1910, I, 319-324.

¹⁹⁴Il Pitagora, Palermo, 17, 1910-11, 31-33.

¹⁹⁵Proc. Cambr. Phil. Soc., 16, 1911, 12.

¹⁹⁶L'intermédiaire des math., 19, 1912, 241-2.

¹⁹⁷Revista de la Sociedad Mat. Española, 2, 1912, 17-21.

¹⁹⁸Periodico di Mat., 29, 1913, 126-8.

¹⁹⁹Math. és Termés Értésítő, 34, 1916, 62-70.

NUMBER OF PRIMES BETWEEN ASSIGNED LIMITS.

Formula (5) of Legendre in Ch. V implies that if θ, λ, \dots are the primes $\leq \sqrt{n}$, the number of primes $\leq n$ and $> \sqrt{n}$ is one less (if unity be counted a prime) than

$$n - \Sigma \left[\frac{n}{\theta} \right] + \Sigma \left[\frac{n}{\theta\lambda} \right] - \dots$$

Statements or proofs of this result have been given by C. J. Hargreave,²⁰⁵ E. de Jonquières,²⁰⁶ R. Lipschitz,²⁰⁷ J. J. Sylvester,²⁰⁸ E. Catalan,²⁰⁹ F. Rogel,²¹⁰ J. Hammond²¹¹ with a modification, H. W. Curjel,^{211a} S. Johnsen,²¹² and L. Kronecker.²¹³

E. Meissel²¹⁴ proved that if $\theta(m)$ is the number of primes (including unity) $\leq m$ and if

$$\Phi(p_1^{n_1} \dots p_m^{n_m}) = (-1)^{n_1 + \dots + n_m} \frac{(n_1 + n_2 + \dots + n_m)!}{n_1! \dots n_m!},$$

$$1 = \Phi(1)\theta\left[\frac{m}{1}\right] + \Phi(2)\theta\left[\frac{m}{2}\right] + \dots + \Phi(m)\theta\left[\frac{m}{m}\right].$$

E. Meissel²¹⁵ wrote $\Phi(m, n)$ for Legendre's formula for the number of integers $\leq m$ which are divisible by no one of the first n primes $p_1 = 2, \dots, p_n$. Then

$$\Phi(m, n) = \Phi(m, n-1) - \Phi\left(\left[\frac{m}{p_n}\right], n-1\right).$$

Let $\theta(m)$ be the number of primes $\leq m$. Set $n + \mu = \theta(\sqrt{m})$, $n = \theta(\sqrt[3]{m})$. Then

$$\theta(m) = \Phi(m, n) + n(\mu + 1) + \frac{\mu(\mu-1)}{2} - 1 - \sum_{s=1}^{\mu} \theta\left(\frac{m}{p_{n+s}}\right),$$

which is used to compute $\theta(m)$ for $m = k \cdot 10^6$, $k = 1/2, 1, 10$.

Meissel²¹⁶ applied his last formula to find $\theta(10^8)$.

Lionnet^{216a} stated that the number of primes between A and $2A$ is $< \theta(A)$.

N. V. Bougaief²¹⁷ obtained from $\theta(n) + \theta(n/2) + \theta(n/3) + \dots = \Sigma[n/p]$, by inversion (Ch. XIX),

$$\theta(x) = \Sigma \left[\frac{n}{a} \right] - 2\Sigma \left[\frac{n}{ab} \right] + 3\Sigma \left[\frac{n}{abc} \right] - \dots - \Sigma \left[\frac{n}{a^2} \right] + \Sigma \left[\frac{n}{a^2b} \right] - \Sigma \left[\frac{n}{a^2bc} \right] + \dots,$$

where a, b, \dots range over all primes.

²⁰⁵Lond. Ed. Dub. Phil. Mag., (4), 8, 1854, 118-122.

²⁰⁶Comptes Rendus Paris, 95, 1882, 1144, 1343; 96, 1883, 231.

²⁰⁷*Ibid.*, 95, 1882, 1344-6; 96, 1883, 58-61, 114-5, 327-9.

²⁰⁸*Ibid.*, 96, 1883, 463-5; Coll. Math. Papers, 4, p. 88.

²⁰⁹Mém. Soc. Roy. Sc. de Liège, (2), 12, 1885, 119; Mélanges Math., 1868, 133-5.

²¹⁰Archiv Math. Phys., (2), 7, 1889, 381-8.

²¹¹Messenger Math., 20, 1890-1, 182.

^{211a}Math. Quest. Educ. Times, 67, 1897, 27.

²¹²Nyt Tidsskrift for Mat., Kjøbenhavn, 15 A, 1904, 41-4.

²¹³Vorlesungen über Zahlentheorie, I, 1901, 301-4.

²¹⁴Jour. für Math., 48, 1854, 310-4.

²¹⁵Math. Ann., 2, 1870, 636-642. Outline in Mathews' Theory of Numbers, 273-8, and in G.

Wertheim's Elemente der Zahlentheorie, 1887, 20-25.

²¹⁶*Ibid.*, 3, 1871, 523-5. Corrections, 21, 1883, 304.

^{216a}Nouv. Ann. Math., 1872, 190. Cf. Landau, (4), 1, 1901, 281-2.

²¹⁷Bull. sc. math. astr., 10, I, 1876, 16. Mat. Sbornik (Math. Soc. Moscow), 6, 1872-3, I, 180.

P. de Mondésir²¹⁸ wrote N_p for the number of multiples of the prime p which are $< 2N$ and divisible by no prime $< p$. Then the number of primes $< 2N$ is $N - \sum N_p + n + 1$, where n is the number of primes $< \sqrt{2N}$. Also,

$$N_p = \left[\frac{N}{p} \right] - \sum \left[\frac{N}{ap} \right] + \sum \left[\frac{N}{abp} \right] - \dots,$$

where a, b, \dots are the primes $< p$. By this modification of Legendre's formula, he computed the number 78490 of primes under one million.

*L. Lorenz²¹⁹ discussed the number of primes under a given limit.

Paolo Paci²²⁰ proved that the number of integers $\leq n$ divisible by a prime $< \sqrt{n}$ is

$$N = \sum \left[\frac{n}{r} \right] - \sum \left[\frac{n}{rs} \right] + \dots \pm \left[\frac{n}{2 \cdot 3 \cdot 5 \dots p} \right],$$

where r, s, \dots range over all the H primes $2, 3, \dots, p$ less than \sqrt{n} . Thus there are $n - 1 - N + H$ primes from 1 to n . The approximate value of N is

$$n \left\{ \sum \frac{1}{r} - \sum \frac{1}{rs} + \dots \right\} = n \left\{ 1 - \frac{\phi(2 \cdot 3 \dots p)}{2 \cdot 3 \dots p} \right\}.$$

K. E. Hoffmann²²¹ denoted by N the number of primes $< m$, by λ the number of distinct prime factors of m , by μ the number of composite integers $< m$ and prime to m . Evidently $N = \phi(M) - \mu + \lambda$. To find N it suffices to determine μ . To that end he would count the products $< m$ by twos, by threes, etc. (with repetitions) of the primes not dividing m .

J. P. Gram²²² proved that the number of powers of primes $\leq n$ is

$$P(n) = \sum \left[\frac{n}{a} \right] - 2 \sum \left[\frac{n}{ab} \right] + 3 \sum \left[\frac{n}{abc} \right] - \dots$$

[Cf. Bougaief.²¹⁷] Of the two proofs, one is by inversion from

$$P(n) + P\left(\frac{n}{2}\right) + P\left(\frac{n}{3}\right) + \dots = \sum \left[\frac{n}{p} \right] + \sum \left[\frac{n}{p^2} \right] + \sum \left[\frac{n}{p^3} \right] + \dots$$

E. Cesàro²²³ considered the number x of primes $\leq qn$ and $> n$, where q is a fixed prime. Let $\omega_1, \dots, \omega_s$ be the primes $\leq n$ other than 1 and q . Let $q^k \leq n < q^{k+1}$. Then

$$k + 2 + x = qn - \sum \left[\frac{qn}{\omega_1} \right] + \sum \left[\frac{qn}{\omega_1 \omega_2} \right] - \dots$$

Let $l_{r,s}$ be the number of the $[qn/(\omega_1 \dots \omega_s)]$ which give the remainder r when divided by q . Set $t_s = \sum j l_{j,s}$. Then

$$x = (k+1)q - (k+2) - t_1 + t_2 - t_3 + \dots$$

²¹⁸Assoc. franç. av. sc., 6, 1877, 77-92. Nouv. Corresp. Math., 6, 1880, 256.

²¹⁹Tidsskr. for Math., Kjobenhavn, (4), 2, 1878, 1-3.

²²⁰Sul numero de numeri primi inferiori ad un dato numero, Parma, 1879, 10 pp.

²²¹Archiv Math. Phys., 64, 1879, 333-6.

²²²K. Danske Vidensk. Selskabs. Skrifter, (6), 2, 1881-6, 183-288; résumé in French, 289-308.

See pp. 220-8, 296-8.

²²³Mém. Soc. Sc. Liège, (2), 10, 1883, 287-8.

E. Catalan²²⁴ obtained the preceding results for the case $q=2$; then t_1 is the number of odd quotients $[2n/\beta]$, t_2 the number of odd quotients $[2n/(\beta\gamma)]$, \dots , where β, γ, \dots are the primes >2 and $\leq n$.

L. Gegenbauer²²⁵ gave eight formulas, (29)–(36), of the type of Legendre's, a special case of one being

$$\sum_x S_k \left(\left[\frac{n}{x} \right] \right) \mu(x) = 1 + L_k(n), \quad S_k(n) \equiv \sum_{t=1}^n t^k,$$

where x ranges over the integers divisible by no prime $> \sqrt{n}$, while $\mu(x)$ is Merten's function (Ch. XIX) and $L_k(n)$ is the sum of the k th powers of all primes $> \sqrt{n}$ but $\leq n$. The case $k=0$ is Legendre's formula. The case $k=1$ is Sylvester's²⁰⁸

E. Meissel²²⁶ computed the number of primes $< 10^9$.

Gegenbauer^{226a} gave complicated expressions for $\theta(n)$, one a generalization of Bougaief's.²¹⁷

A. Lugli²²⁷ wrote $\phi(n, i)$ for the number of integers $\leq n$ which are divisible by no one of the first i primes $p_1=2, p_2=3, \dots$. If i is the number of primes $\leq \sqrt{n}$ and if s is the least integer such that

$$s-1 = \psi[\sqrt{n/p_s}],$$

the number $\psi(n)$ of primes $\leq n$, excluding 1, is proved to satisfy

$$\psi(n) = \left[\frac{n}{2} \right] - \sum_{j=2}^{s-1} \phi \left(\left[\frac{n}{p_j} \right], j-1 \right) - \sum_{j=s}^i \psi \left[\frac{n}{p_j} \right] + \frac{1}{2}(i^2 - s^2 - i + 5s + 6).$$

This method of computing $\psi(n)$ is claimed to be simpler than that by Legendre or Meissel.

J. J. van Laar^{227a} found the number of primes < 30030 by use of the primes < 1760 .

C. Hossfeld²²⁸ gave a direct proof of

$$\Phi(gp_1 \dots p_n \pm r, n) = g(p_1-1) \dots (p_n-1) \pm \Phi(r, n),$$

the case of the upper signs being due to Meissel.²¹⁵

F. Rogel²²⁹ gave a modification and extension of Meissel's²¹⁵ formula.

H. Scheffler²³⁰ discussed the number of primes between p and q .

J. J. Sylvester²³¹ stated that the number of primes $> n$ and $< 2n$ is

$$n - \Sigma H \frac{n}{a} + \Sigma H \frac{n}{ab} - \Sigma H \frac{n}{abc} + \dots,$$

if a, b, \dots are the primes $\leq \sqrt{2n}$ and Hx denotes x when its fractional part

²²⁴Mém. Soc. Sc. Liège, Mém. No. 1.

²²⁵Sitzungsber. Ak. Wiss. Wien (Math.), 89, II, 1884, 841–850; 95, II, 1887, 291–6.

²²⁶Math. Annalen, 25, 1885, 251–7.

^{216a}Sitzungsber. Ak. Wiss. Wien (Math.), 94, II, 1886, 903–10.

²²⁷Giornale di Mat., 26, 1888, 86–95.

^{227a}Nieuw Archief voor Wisk., 16, 1889, 209–214.

²²⁸Zeitschrift Math. Phys., 35, 1890, 382–4.

²²⁹Math. Annalen, 36, 1890, 304–315.

²³⁰Beiträge zur Zahlentheorie, 1891, 187.

²³¹Lucas, Théorie des nombres, 1891, 411–2. Proof by H. W. Curjel, Math. Quest. Educ.

Times, 57, 1892, 113.

is $1/2$, but the nearest integer to x in the contrary case. L. Gegenbauer^{231a} gave a proof and generalization.

Sylvester^{231b} noted that, if $\theta(u)$ is the number of primes $\leq u$, and if p_1, \dots, p_i be the primes $\leq \sqrt{x}$, and q_1, \dots, q_j those between \sqrt{x} and x , then $\Sigma \theta(x/p) - \Sigma \theta(x/q) = \{\theta(\sqrt{x})\}^2$.

H. W. Curjel^{231c} noted that the number of primes $> p$ and $< p^2$ is $\geq p$ if p is a prime ≥ 5 . We have only to delete from $1, 2, \dots, p^2$ multiples of $2, 3, 5, \dots$, or p .

L. Gegenbauer²³² considered the integers x divisible by no square and formed of the odd primes $\leq m$, when $n \geq m \geq \sqrt{2n}$. Of the numbers $[2n/x]$ which are of one of the forms $4s+1$ and $4s+2$, count those in which x is formed of an even number of primes and those in which x is formed of an odd number; denote the difference of the counts by α . He stated that the interval from $m+1$ to n (limits included) contains $\alpha-1$ more primes than the interval from $n+1$ to $2n$.

He gave (pp. 89-93) an expression for the sum of the values taken by an arbitrary function $g(x)$ when x ranges over the primes among the first n terms of an arithmetical progression; in particular, he enumerated the primes $\leq n$ of the form $4s+1$ or $4s-1$.

F. Graefe²³³ would find the number of primes $< m = 10000$ by use of tables showing for each prime p , $5 \leq p \leq \sqrt{m}$, the values of n for which $6n+1$ or $6n+5$ is divisible by p .

P. Bachmann²³⁴ quoted de Jonquières,²⁰⁶ Lipschitz,²⁰⁷ Sylvester,²⁰⁸ and Cesàro.²²³

H. von Koch²³⁵ wrote $f(x) = (x-1)(x-2)\dots(x-n)$,

$$\theta(x) = \prod_{\lambda=2}^n \left\{ 1 - \frac{\rho(x)}{\lambda} \right\}, \quad \rho(x) = \sum_{\mu, \nu=2} \frac{f(x)}{(x-\mu\nu)f'(\mu\nu)} \quad (\mu\nu \leq n),$$

and proved that, for positive integers $x \leq n$, $\theta(x) = 1$ or 0 according as x is prime or composite. The number of primes $\leq m \leq n$ is $\theta(1) + \dots + \theta(m)$.

A. Baranowski²³⁶ noted the formula, simpler than Meissel's,²¹⁵

$$\psi(n) = \phi[n, \psi(\sqrt{n})] + \psi(\sqrt{n}) - 1$$

for computing the number $\psi(n)$ of primes $\leq n$.

S. Wigert^{236a} noted that the number of primes $< n$ is

$$\frac{1}{2\pi i} \int \frac{f'(x)dx}{f(x)}, \quad \text{where } f(x) = \sin^2 \pi x + \sin^2 \pi \left(\frac{1+\Gamma(x)}{x} \right),$$

^{231a}Denkschr. Akad. Wiss. Wien (Math.), 60, 1893, 47.

^{231b}Math. Quest. Educ. Times, 56, 1892, 67-8.

^{231c}*Ibid.*, 58, 1893, 127.

²³²Monatshefte Math. Phys., 4, 1893, 98.

²³³Zeitschrift Math. Phys., 39, 1894, 38-50.

²³⁴Die Analytische Zahlentheorie, 1894, 322-5.

²³⁵Comptes Rendus Paris, 118, 1894, 850-3.

²³⁶Bull. Int. Ac. Sc. Cracovie, 1894, 280-1 (German). Cf. *Rozprawy Akad. Umiej., Cracovie, (2), 8, 1895, 192-219.

^{236a}Öfversigt K. Vetensk. Ak. Förhand., Stockholm, 52, 1895, 341-7.

since the only real zeros of $f(x)$ are the primes. The integration extends over a closed contour enclosing the segment of the x -axis from 1 to n and narrow enough to contain no complex zero of $f(x)$.

T. Levi-Civita^{236b} gave an analytic formula, involving definite integrals and infinite series, for the number of primes between α and β .

L. Gegenbauer²³⁷ gave formulas, similar to that by von Koch,²³⁵ for the number of primes $4s \pm 1$ or $6s \pm 1$ which are $\leq n$.

A. P. Minin^{237a} wrote $\psi(y) = 0$ or 1 according as y is composite or prime; then

$$\theta(n-1) = [n-2] + [n-5] + [n-7] + \dots - \Sigma \psi(x-1)[n-x],$$

summed for all composite integers x .

Gegenbauer^{237b} proved that Sylvester's²³¹ expression for the number of primes $> n$ and $< 2n$ equals $\Sigma \mu(x)[m/x + 1/2]$, where x takes those integral values $\leq 2n$ which are products of primes $\leq \sqrt{2n}$.

F. Rogel²³⁸ gave a recursion formula for the number of primes $\leq m$.

T. Hayashi²³⁹ wrote Rf/q for the remainder obtained on dividing f by q . By Laurent's¹⁸⁷ result, $-RF_n(x)/(x^n-1)n^{n-2} = 0$ or 1 according as n is composite or prime. Hence the sum of the j th powers of the primes between s and t is

$$-R \sum_{n=s}^t \frac{F_n(x)}{(x^n-1)n^{n-j-2}},$$

which becomes the number of primes for $j=0$. If α is a primitive n th root of unity, Wilson's theorem shows that

$$\sum_{j=0}^{n-1} \alpha^{jm} = n \text{ or } 0 \quad (m = (n-1)! + 1),$$

according as n is prime or composite. Hence $Rx^{(n-1)!}/(x^n-1) = 1$ or 0 according as n is prime or composite. Thus

$$R \sum_{n=s}^t x^{(n-1)!}/(x^n-1)$$

is the number of primes between s and t .

Hayashi²⁴⁰ reproduced the second of his two preceding results and gave it the form

$$\int_0^{2\pi} r^{n-m} \frac{\{\cos(m-n)\theta - r^n \cos m\theta\} d\theta}{1 - 2r^n \cos n\theta + r^{2n}} = 2\pi \text{ or } 0,$$

according as n is prime or not, and gave a direct proof.

J. V. Pexider²⁴¹ investigated the number $\psi(x)$ of primes $\leq x$. Write

$$\Delta \left[\frac{n}{\mu} \right] = \left[\frac{n}{\mu} \right] - \left[\frac{n-1}{\mu} \right], \quad \delta_\mu = \Delta \left[\frac{ak}{\mu} \right].$$

^{236b}Atti R. Accad. Lincei, Rendiconti, (5), 4, 1895, I, 303-9.

²³⁷Monatshefte Math. Phys., 7, 1896, 73.

^{237a}Bull. Math. Soc. Moscow, 9, 1898, No. 2; Fortschritte, 1898, 165.

^{237b}Monatshefte Math. Phys., 10, 1899, 370-3.

²³⁸Archiv Math. Phys., (2), 17, 1900, 225-237.

²³⁹Jour. of the Phys. School in Tokio, 9, 1900; reprinted in Abhand. Gesch. Math. Wiss., 28, 1900, 72-5.

²⁴⁰Archiv Math. Phys., (3), 1, 1901, 246-251.

²⁴¹Mitt. Naturforsch. Gesell. Bern, 1906, 82-91.

Hence the number of integers $\leq x$ which are divisible by a , but not by $a-1, a-2, \dots, 2$, is

$$\sigma_a = \sum_{k=1}^{\lfloor x/a \rfloor} \prod_{\mu=2}^{a-1} (1 - \delta_\mu).$$

The number $\Psi(x)$, of primes $\leq x$ and $> \nu = [\sqrt{x}]$ is $[x] - 1 - \sum_{a=2}^{\nu} \sigma_a$. Let p_1, \dots, p_a be the primes $\leq \sqrt{a}$. Let p_ω be the greatest prime $\leq \nu$. Then

$$\Psi(x) + 1 = [x] - \left[\frac{x}{2} \right] - \sum_{a=3}^{\omega} \sum_{k=1}^{\lfloor x/p_a \rfloor} \prod_{\mu=2}^{a-1} \left\{ 1 - \Delta \left[\frac{p_a^k}{p_\mu} \right] \right\},$$

from which follows Legendre's formula.

S. Minetola²⁴² obtained a formula to compute the number of primes $\leq K = 2k+1$, not presupposing a knowledge of any primes > 2 , by considering the sets of positive integers n, n', \dots for which

$$(2n+1)(2n'+1) \leq K, \quad (2n+1)(2n'+1)(2n''+1) \leq K, \dots$$

F. Rogel²⁴³ started with Legendre's formula for the number $A(z)$ of primes $\leq z$, introduced the remainders $t - |t|$, and wrote $R_n(z)$ for the sum of these partial remainders. He obtained relations between values of the A 's and R 's for various arguments z , and treated sums of such values. For arbitrary x 's (p. 1815),

$$\sum_{\nu=1}^{p_{n+1}-1} (x_{\nu+1} - x_\nu) A(\nu) = -\sum x_p + x_{p_{n+1}} A(p_n),$$

summed for the primes p between 1 and the n th prime p_n . By special choice of the x 's, we get formulas involving Euler's ϕ -function (p. 1818), and the number or sum of the divisors of an integer. See Rogel²⁴² of Ch. XI.

G. Andreoli²⁴⁴ noted that, if x is real, and Γ is the gamma function,

$$\Phi(x) = \sin^2 \frac{(\Gamma(x)+1)\pi}{x} + \sin^2 \pi x$$

is zero if and only if x is a prime. Hence the number of primes $< n$ is

$$\frac{1}{2\pi i} \int_1^n \frac{\Phi'(x) dx}{\Phi(x)}.$$

The sum of the k th powers of the primes $< n$ is given asymptotically.

M. Petrovitch²⁴⁵ used a real function $\theta(x, u)$, like

$$a \cos 2\pi x + b \cos 2\pi u - a - b,$$

which is zero for every pair of integers x, u , and not if x or u is fractional. Let $\Phi(x)$ be the function obtained from $\theta(x, u)$ by taking

$$u = \{1 + \Gamma(x)\} / x.$$

Thus $y = \Phi(x)$ cuts the x -axis in points whose abscissas are the primes.

²⁴²Giornale di Mat., 47, 1909, 305-320.

²⁴³Sitzungsber. Ak. Wiss. Wien (Math.), 121, 1912, IIa, 1785-1824; 122, 1913, IIa, 669-700.

²⁴⁴Rendiconti Accad. Lincei, (5), 21, II, 1912, 404-7. Wigert.^{238a}

²⁴⁵Nouv. Ann. Math., (4), 13, 1913, 406-10.

E. Landau²⁴⁶ indicated errors in l'intermédiaire des mathématiciens on the approximate number of primes $ax+b < N$.

*M. Kössler²⁴⁷ discussed the relation between Wilson's theorem and the number of primes between two limits.

See Cesàro⁶⁴ of Ch. V, Gegenbauer¹² of Ch. XI, and papers 62-81 of Ch. XIII.

BERTRAND'S POSTULATE.

J. Bertrand²⁶⁰ verified for numbers $< 6\,000\,000$ that for any integer $n > 6$ there exists at least one prime between $n-2$ and $n/2$.

P. L. Tchebychef²⁶¹ obtained limits for the sum $\theta(z)$ of the natural logarithms of all primes $\leq z$ and deduced Bertrand's postulate that, for $x > 3$, there exists a prime between x and $2x-2$. His investigation shows that for every $\epsilon > 1/5$ there exists a number ξ such that for every $x \geq \xi$ there exists at least one prime between x and $(1+\epsilon)x$.

A. Desboves,²⁶² assuming an unproved theorem of Legendre's,²² concluded the existence of at least two primes between any number > 6 and its double, also between the squares of two consecutive primes; also at least p primes between $2n$ and $2n-k$ for p and k given and n sufficiently large, and hence between a sufficiently large number and its square.

F. Proth²⁶³ claimed to prove Bertrand's postulate.

J. J. Sylvester²⁶⁴ reduced Tchebychef's ϵ to 0.16688.

L. Oppermann²⁶⁵ stated the unproved theorem that if $n > 1$ there exists at least one prime between $n(n-1)$ and n^2 , and also between n^2 and $n(n+1)$, giving a report on the distribution of primes.

E. C. Catalan²⁶⁶ proved that Bertrand's postulate is equivalent to

$$\frac{(2n)!}{n! \, n!} > \alpha^a \beta^b \dots \pi^p,$$

where α, \dots, π denote the primes $\leq n$, while a is the number of odd integers among $[2n/\alpha]$, $[2n/\alpha^2], \dots$, b the number among $[2n/\beta]$, $[2n/\beta^2], \dots$. He noted (p. 31) that if the postulate is applied to $b-1$ and $b+1$, we see the existence between $2b$ and $4b$ of at least one even number equal to the sum of two primes.

J. J. Sylvester²⁶⁷ reduced Tchebychef's ϵ to 0.092; D. von Sterneck²⁶⁸ to 0.142.

²⁴⁶L'intermédiaire des math., 20, 1913, 179; 15, 1908, 148; 16, 1909, 20-1.

²⁴⁷Casopis, Prag, 44, 1915, 38-42.

²⁶⁰Jour. de l'école roy. polyt., cah. 30, tome 17, 1845, 129.

²⁶¹Mém. Ac. Sc. St. Pétersbourg, 7, 1854 (1850), 17-33, 27; Oeuvres, 1, 49-70, 63. Jour. de Math., 17, 1852, 366-390, 381. Cf. Serret, Cours d'algèbre supérieure, ed. 2, 2, 1854, 587; ed. 6, 2, 1910, 226.

²⁶²Nouv. Ann. Math., 14, 1855, 281-295.

²⁶³Nouv. Corresp. Math., 4, 1878, 236-240.

²⁶⁴Amer. Jour. Math., 4, 1881, 230.

²⁶⁵Oversigt Videnskabs Selsk. Forh., 1882, 169.

²⁶⁶Mém. Soc. R. Sc. Liège, (2), 15, 1888 (= Mélanges Math., III), 108-110.

²⁶⁷Messenger Math., (2), 21, 1891-2, 120.

²⁶⁸Sitzungsb. Akad. Wiss. Wien, 109, 1900, IIa, 1137-58.

T. J. Stieltjes stated and E. Cahen²⁶⁹ proved that we may take ϵ to be any positive number however small, since $\theta(z)$ is asymptotic³¹⁵⁻⁶ to z .

H. Brocard²⁷⁰ stated that at least four primes lie between the squares of two consecutive primes, the first being >3 . He remarked that this and the similar theorem by Desboves²⁶² can apparently be deduced from Bertrand's postulate; but this was denied by E. Landau.²⁷¹

E. Maillet²⁷² proved there is at least one prime between two consecutive squares $<9 \cdot 10^6$ or two consecutive triangular numbers $\leq 9 \cdot 10^6$.

E. Landau⁴⁷ (pp. 89-92) proved Bertrand's postulate and hence the existence of a prime between x (excl.) and $2x$ (incl.) for every $x \geq 1$.

A. Bonolis²⁷³ proved that, if $x > 13$ is a number of p digits and a is the least integer $> x/\{10(p+1)\}$, there exist at least a primes between x and $[\frac{3}{2}x-2]$, which implies Bertrand's postulate. If $x > 13$ is a number of p digits and β is the greatest integer $< x/(3p-3)$, there are fewer than β primes from x to $[\frac{3}{2}x-2]$.

MISCELLANEOUS RESULTS ON PRIMES.

H. F. Scherk²⁸⁰ stated the empirical theorems: Every prime of odd rank (the n th prime 1, 2, 3, 5, ... being of rank n) can be composed by addition and subtraction of all the smaller primes, each taken once; thus

$$13 = 1 + 2 - 3 - 5 + 7 + 11 = -1 + 2 + 3 + 5 - 7 + 11.$$

Every prime of even rank can be composed similarly, except that the next earlier prime is doubled; thus

$$17 = 1 + 2 - 3 - 5 + 7 - 11 + 2 \cdot 13 = -1 - 2 + 3 - 5 + 7 - 11 + 2 \cdot 13.$$

Märcker²⁸¹ noted that, if a, b, \dots, m are the primes between 1 and A and if p is their product, all the primes from A to A^2 are given by

$$p \left(\frac{a}{a} + \frac{\beta}{b} + \dots + \frac{\mu}{m} + n \right),$$

and each but once if each numerator is positive and less than its denominator.

O. Terquem²⁸² noted that the primes $< n^2$ are the odd numbers not included in the arithmetical progressions $q^2, q^2+2q, q^2+4q, \dots$ up to n^2 , for $q=3, 5, \dots, n-1$.

H. J. S. Smith²⁸³ gave a theoretical method of finding the primes between the x th prime P_x and P_{x+1}^2 , given the first x primes.

C. de Polignac^{283a} considered the primes $\leq x$ in a progression $Km+h$.

²⁶⁹Comptes Rendus Paris, 116, 1893, 490; Thèse, 1894, 45; Ann. École Normale, (3), 11, 1894.

²⁷⁰L'intermédiaire des math., 11, 1904, 149.

²⁷¹Ibid., 20, 1913, 177.

²⁷²Ibid., 12, 1905, 110-3.

²⁷³Atti Ac. Sc. Torino, 47, 1911-12, 576-585.

²⁸⁰Jour. für Math., 10, 1833, 201.

²⁸¹Ibid., 20, 1840, 350.

²⁸²Nouv. Ann. Math., 5, 1846, 609.

²⁸³Proc. Ashmolean Soc., 3, 1857, 128-131; Coll. Math. Papers, 1, 37.

^{283a}Comptes Rendus Paris, 54, 1862, 158-9.

E. Dormoy²⁸⁴ noted that, if $2, 3, \dots, r, s, t, u$ are the primes in natural order, all primes (and no others) $< u^2$ are given by

$$2 \cdot 3 \dots stm + D_t a_t + t C_t D_s a_s + ts C_t C_s D_r a_r + \dots \\ + tsr \dots 7 \cdot 5 C_t C_s C_r \dots C_5 D_3 a_3 + ts \dots 5 \cdot 3 C_t C_s \dots C_3,$$

where C_t is found from the quotients obtained in finding the g. c. d. of t and $2 \cdot 3 \dots rs$ by a rule which if applied to four quotients a, b, c, d consists in forming in turn $1, p = dc + 1, pb + d, (pb + d)a + p = C_t$. Further, $D_t = tC_t \pm 1$, the sign being $+$ or $-$ according as there is an odd or an even number of operations in the g. c. d. process.

C. de Polignac^{284a} wrote p_n for the n th prime and discussed the expressibility of all numbers, under a specified limit and divisible by no one of p_1, \dots, p_{n-1} , in the form

$$(p_2, p_3, \dots, p_{n-1}, p_n) + (p_3, p_4, \dots, p_n, p_1) + \dots + (p_1, \dots, p_{n-1}),$$

where (a, b, \dots) denotes $\pm a^a b^b \dots$. For example, every number < 53 and divisible by neither 2 nor 3 is of the form $\pm 3^a \pm 2^b$.

J. J. Sylvester²⁸⁵ proved that if m is prime to i and not less than n , the product $(m+i)(m+2i) \dots (m+ni)$ is divisible by some prime $> n$.

A. A. Markow²⁸⁶ found a fragment in a manuscript by Tchebychef aiding him to prove the latter's result that if μ is the greatest prime divisor of $(1+2^2)(1+4^2) \dots (1+4N^2)$, then μ/N increases without limit with N (cf. Hermite, Cours, ed. 4, 1891, 197).

J. Iwanow²⁸⁷ generalized the preceding theorem as follows: If μ is the greatest prime divisor of $(A+1^2) \dots (A+L^2)$, then μ/L increases without limit with L .

C. Störmer²⁸⁸ concluded the existence of an infinitude of primes from Tchebychef's²⁸⁶ result and used the latter to prove that $i(i-1)(i-2) \dots (i-n)$ is neither real nor purely imaginary if n is any integer $\neq 3$, and $i = \sqrt{-1}$.

E. Landau⁴⁷ (pp. 559-564) discussed the topics in the last three papers.

Braun^{13a} proved that the $(n+1)$ th prime is the only root $x \neq 1$ of

$$x \prod_{i=1}^n a_i^{[x/a_i] + [x/a_i^2] + \dots} = x!,$$

where $a_1 = 2, a_2, \dots, a_n$ are the first n primes.

C. Isenkrahe²⁸⁹ expressed a prime in terms of the preceding primes.

R. Le Vavasseur²⁹⁰ noted that all primes between p_n and p_{n+1}^2 , where p_n is the n th prime, are given by $\sum_{i=1}^n q_i w_i P_n / p_i \pmod{P_n}$, where $P_n = p_1 p_2 \dots p_n$ and $w_i P_n / p_i \equiv 1 \pmod{p_i}$.

²⁸⁴Comptes Rendus Paris, 63, 1866, 178-181.

^{284a}Comptes Rendus Paris, 104, 1887, 1688-90.

²⁸⁵Messenger Math., 21, 1891-2, 1-19, 192. Math. Quest. Educ. Times, 56, 1892, 25.

²⁸⁶Bull. Acad. Sc. St. Pétersbourg, 3, 1895, 55-8.

²⁸⁷Ibid., 361-6.

²⁸⁸Archiv Math. og Natur., Kristiania, 24, 1901-2, No. 5.

²⁸⁹Math. Annalen, 53, 1900, 42.

²⁹⁰Mém. Ac. Sc. Toulouse, (10), 3, 1903, 36-8.

O. Meissner²⁹¹ stated that, if $n+1$ successive integers $m, \dots, m+n$ are given, we can not in general find another set m_1, \dots, m_1+n containing a prime $m_1+\nu$ corresponding to every prime $m+\nu$ of the first set. But for $n=2$, it is supposed true that there exist an infinitude of prime pairs.

G. H. Hardy²⁹² noted that the largest prime dividing a positive integer x is

$$\lim_{r=\infty} \lim_{m=\infty} \lim_{n=\infty} \sum_{\nu=0}^m [1 - (\cos\{(\nu!)^r \pi/x\})^{2n}].$$

C. F. Gauss,²⁹³ in a manuscript of 1796, stated empirically that the number $\pi_2(x)$ of integers $\leq x$ which are products of two distinct primes, is approximately $x \log \log x / \log x$.

E. Landau²⁹⁴ proved this result and the generalization

$$\pi_\nu(x) = \frac{1}{(\nu-1)!} \cdot \frac{x(\log \log x)^{\nu-1}}{\log x} + O\left\{\frac{x(\log \log x)^{\nu-2}}{\log x}\right\},$$

where $\pi_\nu(x)$ is the number of integers $\leq x$ which are products of ν distinct primes; also related formulas for $\pi_\nu(x)$.

Several writers²⁹⁵ gave numerous examples of a sum of consecutive primes equal to an exact power.

E. Landau²⁹⁶ proved that the probability that a number of n digits be a prime, when n increases indefinitely, is asymptotically equal to $1/(n \log 10)$.

J. Barinaga²⁹⁷ expressed the sum of the first n primes as a product of distinct primes for $n=3, 7, 9, 11, 12, 16, 22, 27, 28$, and asked if there is a general law.

Coblyn²⁹⁸ noted as to prime pairs that, when $4(6p-2)!$ is divided by $36p^2-1$, the remainder is $-6p-3$ if $6p-1$ and $6p+1$ are both primes, zero if both are composite, $-2(6p+1)$ if only $6p-1$ is prime, and $6p-1$ if only $6p+1$ is prime.

J. Hammond²⁹⁹ gave formulas connecting the number of odd primes $< 2n$, and the number of partitions of $2n$ into two distinct primes or into two relatively prime composite numbers.

V. Brun³⁰⁰ proved that, however great a is, there exist a successive composite numbers of the form $1+u^2$. There exist a successive primes no two of which differ by 2. He determined a superior limit for the number of primes $< x$ of a given class.

²⁹¹Archiv Math. Phys., 9, 1905, 97.

²⁹²Messenger Math., 35, 1906, 145.

²⁹³Cf. F. Klein, Nachrichten Gesell. Wiss. Göttingen, 1911, 26-32.

²⁹⁴*Ibid.*, 361-381; Handbuch... der Primzahlen, I, 1909, 205-211; Bull. Soc. Math. France, 28, 1900, 25-38.

²⁹⁵L'intermédiaire des math., 18, 1911, 85-6.

²⁹⁶*Ibid.*, 20, 1913, 180.

²⁹⁷L'intermédiaire des math., 20, 1913, 218.

²⁹⁸Soc. Math. de France, C. R. des Séances, 1913, 55.

²⁹⁹Proc. London Math. Soc., (2), 15, 1916-7, Records of Meetings, Feb. 1916, xxvii.

³⁰⁰Nyt Tidsskrift for Matematik, B, 27, 1916, 45-58.

DIATOMIC SERIES.

A. de Polignac³⁰⁵ crossed out the multiples of 2 and 3 from the series of natural numbers and obtained the "table a_2 ":

(0) 1 (2) (3) (4) 5 (6) 7 (8) (9) (10) 11....

The numbers of terms in the successive sets of consecutive deleted numbers are 1, 3, 1, 3, 1, ..., which form the "diatomic series of 3." Similarly, after deleting the multiples of the first n primes, we get a table a_n and the diatomic series of the n th prime P_n . That series is periodic and the terms after 1 of the period are symmetrically distributed (two terms equidistant from the ends are equal), while the middle term is 3. Let π_n denote the product of the primes 2, 3, ..., P_n . Then the number of terms in the period is $\phi(\pi_n)$. The sum of the terms in the period is $\pi_n - \phi(\pi_n)$ and hence is the number of integers $< \pi_n$ which are divisible by one or more primes $\leq P_n$. As applications he stated that there exists a prime between P_n and P_n^2 , also between a^n and a^{n+1} . He³⁰⁶ stated that the middle terms other than 3 of a diatomic series tend as n increases to become 1, 3, 7, 15, ..., $2^m - 1$,

J. Deschamps³⁰⁷ noted that, after suppressing from the series of natural numbers the multiples of the successive primes 2, 3, ..., p , the numbers left form a periodic series of period $2 \cdot 3 \dots p$; and similar theorems. Like remarks had been made previously by H. J. S. Smith.³⁰⁸

ASYMPTOTIC DISTRIBUTION OF PRIMES.

P. L. Tchebychef's²⁶¹ investigation shows that for x sufficiently large the number $\pi(x)$ of primes $\leq x$ is between $0.921Q$ and $1.106Q$, where $Q = x/\log x$. He³¹⁴ proved that the limit, if existent, of $\pi(x)/Q$ for $x = \infty$ is unity. J. J. Sylvester²⁶⁷ obtained by the same methods the limits $0.95Q$ and $1.05Q$.

By use of the function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ of Riemann, J. Hadamard³¹⁵ and Ch. de la Vallée-Poussin³¹⁶ independently proved that the sum of the natural logarithms of all primes $\leq x$ equals x asymptotically. Hence follows the fundamental theorem that $\pi(x)$ is asymptotic to Q , i. e.,

$$\lim_{x=\infty} \pi(x) \cdot \frac{\log x}{x} = 1.$$

³⁰⁵Recherches nouvelles sur les nombres premiers, Paris, 1851, 28 pp. Abstract in Comptes Rendus Paris, 29, 1849, 397-401, 738-9; same in Nouv. Ann. Math., 8, 1849, 423-9. Jour. de Math., 19, 1854, 305-333.

³⁰⁶Nouv. Ann. Math., 10, 1851, 308-12.

³⁰⁷Bull. Soc. Philomathique de Paris, (9), 9, 1907, 102-112

³⁰⁸Proc. Ashmolean Soc., 3, 1857, 128-131; Coll. Math. Papers, 1, 36.

³¹⁴Mém. Ac. Sc. St. Pétersbourg, 6, 1851, 146; Jour. de Math., 17, 1852, 348; Oeuvres, 1, 34.

³¹⁵Bull. Soc. Math. de France, 24, 1896, 199-220.

³¹⁶Annales de la Soc. Sc. de Bruxelles, 20, II, 1896, 183-256.

Now Q is asymptotic to the "integral logarithm of x ":

$$Lix = \lim_{\delta=0} \left(\int_0^{1-\delta} \frac{du}{\log u} + \int_{1+\delta}^x \frac{du}{\log u} \right),$$

so that the latter is asymptotic to $\pi(x)$. De la Vallée-Poussin³¹⁷ proved that Lix represents $\pi(x)$ more exactly than $x/\log x$ and its remaining approximations

$$\frac{x}{\log x} + \frac{x}{\log^2 x} + \dots + \frac{(m-1)!x}{\log^m x}.$$

The history of this extensive subject is adequately presented in the luminous and exhaustive text by E. Landau,⁴⁷ in which is given (pp. 908–961) a complete list of references. The reader may consult the article by J. Hadamard,³¹⁸ the extensive report by G. Torelli,³¹⁹ the summaries by Landau,³²⁰ also G. H. Hardy and J. E. Littlewood,³²¹ and the recent papers 42–44 of Chapter XIX.

³¹⁷Mém. Couronnés Acad. Roy. Belgique, 59, 1889, 1–74.

³¹⁸Encyclopédie des sc. math., tome I, vol. 3, pp. 310–345.

³¹⁹Atti R. Accad. Sc. Fis. Mat., Napoli, (2), 11, 1902, No. 1, 222 pp.

³²⁰Proc. Fifth Internat. Congress, Cambridge, 1, 1913, 93–108. Math. Zeitschrift, 1, 1918, 1–24, 213–9.

³²¹Acta Math., 41, 1917, 119–196.

CHAPTER XIX.

INVERSION OF FUNCTIONS; MÖBIUS' FUNCTION $\mu(n)$; NUMERICAL INTEGRALS AND DERIVATIVES.

INVERSION; FUNCTION $\mu(n)$.

A. F. Möbius¹ defined the function $\mu(n)$ to be zero if n is divisible by a square >1 , but to be $(-1)^k$ if n is a product of k distinct primes >1 , while $\mu(1)=1$. He employed the function in the reversion of series:

$$F(x) = \sum_{s=1}^{\infty} \frac{f(sx)}{s^n} \text{ implies } f(x) = \sum_{s=1}^{\infty} \mu(s) \frac{F(sx)}{s^n}.$$

His results were expressed in more general form by Glaisher⁶⁹ and cited in Chapter X. See also E. Meissel,² who³ noted that

$$(1) \quad \sum_{j=1}^m \mu(j) \left[\frac{m}{j} \right] = 1.$$

R. Dedekind⁴ proved that, if $F(m) = \sum f(d)$, where d ranges over all the divisors of m , then

$$(2) \quad f(m) = F(m) - \sum F\left(\frac{m}{a}\right) + \sum F\left(\frac{m}{ab}\right) - \sum F\left(\frac{m}{abc}\right) + \dots,$$

where the summations extend over all the combinations 1, 2, 3, ... at a time of the distinct prime factors a, b, \dots, k of m . The proof follows from a distribution of all the factors of m into two sets S and T . Put all the divisors of m into set S ; all divisors of m/a into set T , all of m/b into T , etc.; all divisors of $m/(ab)$ into S , all of $m/(ac)$ into S , etc.; all of $m/(abc)$ into T , etc. Then, with the exception of m itself, every divisor of m occurs as often in the set S as in the set T . In particular, for Euler's $\phi(m)$, $m = \sum \phi(d)$, whence

$$\phi(m) = m - \sum \frac{m}{a} + \sum \frac{m}{ab} - \dots = m \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \dots$$

For another example, see Dedekind⁷¹ of Ch. VIII. Similarly, $F(m) = \prod f(d)$ implies

$$f(m) = \frac{F(m) \prod F\left(\frac{m}{ab}\right) \dots}{\prod F\left(\frac{m}{a}\right) \prod F\left(\frac{m}{abc}\right) \dots}$$

J. Liouville⁵ stated simultaneously with Dedekind the inversion theorem for sums and made the same application to $\phi(m)$.

Liouville⁶ stated the theorem for sums as a problem.

¹Jour. für Math., 9, 1832, 105; Werke, 4, 591. He wrote a_n for $\mu(n)$.

²*Ibid.*, 48, 1854, 301-316.

³Observationes quaedam in theoria numerorum, Berlin, 1850, pp. 3-6.

⁴Jour. für Math., 54, 1857, pp. 21, 25.

⁵Jour. de Mathématiques, (2), 2, 1857, 110-2.

⁶Nouv. Ann. Math., 16, 1857, 181-2.

B. Merry⁷ gave a proof by noting that, if d is any divisor of m , and if q of the prime factors of m occur to the same power in d as in m , then $f(d)$ occurs once in $F(m)$, q times in $\Sigma F(m/a)$, $q(q-1)/2$ times in $\Sigma F(m/ab)$, etc. Thus the coefficient of $f(d)$ in (2) is

$$1 - q + \frac{q(q-1)}{1 \cdot 2} - \dots = (1-1)^q = 0$$

if $q > 0$, but is unity if $q = 0$, i. e., if $d = m$. This proof is only another way of stating Dedekind's proof.

R. Dedekind⁸ gave another form and proof of his theorems. Let

$$m \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \dots = \Sigma \nu_1 - \Sigma \nu_2,$$

where ν_1 ranges over the positive terms of the expanded product and $-\nu_2$ over the negative terms. A simple proof shows that, if ν is any divisor $< m$ of m , there are as many terms ν_1 divisible by ν as terms ν_2 divisible by ν . Thus

$$\Sigma f(\nu) = F(m), \quad \Pi f(\nu) = F(m)$$

imply, respectively,

$$f(m) = \Sigma F(\nu_1) - \Sigma F(\nu_2), \quad f(m) = \frac{\Pi F(\nu_1)}{\Pi F(\nu_2)}.$$

Liouville^{8a} wrote $F(n) = \Sigma f(n/D^\mu)$, where D ranges over those divisors of $n = a^\alpha b^\beta \dots$ for which D^μ divides n . Then

$$f(n) = F(n) - \Sigma F(n/a^\mu) + \Sigma F(n/a^\mu b^\mu) - \dots$$

E. Laguerre⁹ expressed (2) in the form

$$(3) \quad f(m) = \Sigma \mu \left(\frac{m}{d} \right) F(d),$$

where d ranges over the divisors of m . Let

$$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} F(n) x^n,$$

whence $F(m) = \Sigma f(d)$. For $m = \Pi p^a$, where the p 's are distinct primes, let $f(m) = \Pi f(p^a)$, and $f(p^n) = p^{n-1}(p-1)$. Then

$$F(m) = \Pi \{1 + f(p) + \dots + f(p^{a-1})\} = \Pi p^a = m.$$

The hypotheses are satisfied if f is Euler's function ϕ . This discussion deduces $\Sigma \phi(d) = m$ from the usual expression of type (3) for $\phi(m)$, rather than the reverse as claimed.

N. V. Bougaief¹⁰ proved (1).

F. Mertens¹¹ defined $\mu(n)$ and noted that $\Sigma \mu(d) = 0$ if $n > 1$, where d ranges over the divisors of n .

⁷Nouv. Ann. Math. 16, 1857, 434.

⁸Dirichlet's Zahlentheorie, mit Zusätzen von Dedekind, 1863, §138; ed. 2, 1871, p. 356; ed. 4, 1894, p. 360.

^{8a}Jour. de Math., (2), 8, 1863, 349.

⁹Bull. Soc. Math. France, 1, 1872-3, 77-81.

¹⁰Mat. Sbornik (Math. Soc. Moscow), 6, 1872-3, 179. Cf. Sterneek.¹¹

¹¹Jour. für Math., 77, 1874, 289; 78, 1874, 53.

E. Cesàro¹² proved formulas, quoted in Ch. X, which include (3) as a special case. His erroneous evaluation of the mean of $\mu(n)$ is cited there.

Cesàro¹³ reproduced the general formula just cited and extended it to three pairs of functions:

$$\begin{aligned}\Sigma f_1(d)F_1\left(\frac{n}{d}\right) &= \Sigma f_2(d)F_2\left(\frac{n}{d}\right) = \Sigma f_3(d)F_3\left(\frac{n}{d}\right), \\ F_1(n) &= \Sigma f_2(d)f_3\left(\frac{n}{d}\right), & F_2 &= \Sigma f_3f_1, & F_3 &= \Sigma f_1f_2.\end{aligned}$$

where, in each, d ranges over the divisors of n .

Cesàro¹⁴ noted that, if $h(n) + k(n) = 1$ and

$$H(n) = h(p)h(q)\dots, \quad K(n) = k(p)k(q)\dots,$$

where p, q, \dots are the prime factors of n , then

$$H(n) = \Sigma \mu(d)K(d), \quad K(n) = \Sigma \mu(d)H(d).$$

For $h(n) = k(n) = 1/2$, then $H(n) = K(n)$ is the reciprocal of the number of divisors, without square factors, of n .

Cesàro¹⁵ treated the inversion of series. Let $\Omega(x) = 1$ or 0 , according as x is or is not in a given set Ω of integers. Let $\Omega(x)\Omega(y) = \Omega(xy)$. Let $\epsilon_\alpha(x)$ be functions such that $\epsilon_\alpha\{\epsilon_\beta(x)\} = \epsilon_{\alpha\beta}(x)$ for every pair of indices α, β . Then

$$F(x) = \Sigma_{\omega} h(\omega) f\{\epsilon_{\omega}(x)\},$$

where ω ranges over all the numbers of Ω , implies that

$$f(x) = \Sigma_{\omega} H(\omega) F\{\epsilon_{\omega}(x)\},$$

if the sum $\Sigma h(d)H(n/d)$, for d ranging over the divisors of n , equals 1 or 0 according as $n = 1$ or $n > 1$. Cf. Möbius¹.

N. V. Bougaief¹⁶ considered the function $\nu(x)$ with the value $\log p$ if x is a power of a prime p , the value 0 in all other cases. Then, if d ranges over the divisors of n , $\Sigma \nu(d) = \log n$ implies $\Sigma \mu(d) \log d = -\nu(n)$.

H. F. Baker¹⁷ gave a generalization of the inversion formula, the statement of which will be clearer after the consideration of one of his applications of it. Let a_1, \dots, a_n be distinct primes and S any set of positive integers. For $k \leq n$, let $F(a_1, \dots, a_k)$ denote the set of all the numbers in S which are divisible by each of the primes $a_{k+1}, a_{k+2}, \dots, a_n$, so that $F(a_1, \dots, a_n) = S$. For $k = 0$, write $F(0)$ for F , so that $F(0)$ consists of the numbers of S which are divisible by a_1, \dots, a_n . Returning to the general $F(a_1, \dots, a_k)$, we divide it into sub-sets. Those of its numbers which are divisible by no one of a_1, \dots, a_k form the sub-set $f(a_1, \dots, a_k)$. Those divisible by a_1 , but by no one of a_2, \dots, a_k , form the sub-set $f(a_2, a_3, \dots, a_k)$.

¹²Mém. soc. roy. sc. de Liège, (2), 10, 1883, No. 6, pp. 26, 47, 56-8.

¹³Giornale di Mat., 23, 1885, 168 (175).

¹⁴Ibid., 25, 1887, 14-19. Cf. 1-13 for a type of inversion formulas.

¹⁵Annali di Mat., (2), 13, 1885, 339; 14, 1886-7, 141-158.

¹⁶Comptes Rendus Paris, 106, 1888, 652-3. Cf. Cesàro, *ibid.*, 1340-3; Cesàro,¹² pp. 315-320; Bougaief, Mat. Sbornik (Math. Soc. Moscow), 13, 1886-8, 757-77; 14, 1888-90, 1-44, 169-201; 18, 1896, 1-54; Kronecker³⁰ (p. 276); Berger^{17a} (pp. 106-115); Gegenbauer¹² of Ch. XI—all on $\Sigma \mu(d) \log d$.

¹⁷Proc. London Math. Soc., 21, 1889-90, 30-32.

Those divisible by a_1 and a_2 , but by no one of a_3, \dots, a_k , form the sub-set $f(a_3, \dots, a_k)$. Finally, those divisible by a_1, \dots, a_k form the sub-set designated $f(0)$. Thus

$$F(a_1, a_2, \dots, a_k) = f(a_1, a_2, \dots, a_k) + \sum_1 f(a_2, a_3, \dots, a_k) + \sum_2 f(a_3, a_4, \dots, a_k) \\ + \dots + \sum_{n-1} f(a_1) + f(0),$$

where \sum indicates that the summation extends over all combinations of a_1, \dots, a_r taken* $k-r$ at a time.

When we have any such set or function $f(a_1, \dots, a_k)$, uniquely determined by a_1, \dots, a_k , independently of their order, and we define F by the foregoing formula, then we have the inverse formula

$$f(a_1, a_2, \dots, a_n) = F(a_1, a_2, \dots, a_n) - \sum_1 F(a_2, a_3, \dots, a_n) + \sum_2 F(a_3, a_4, \dots, a_n) \\ - \dots + (-1)^{n-1} \sum_{n-1} F(a_1) + (-1)^n F(0),$$

where \sum now indicates that the summation extends over all the combinations of a_1, \dots, a_n taken $n-r$ at a time. The proof is just like that by B. Merry for Dedekind's formula.

To give an example, let $n=2$, $a_1=2$, $a_2=3$, $S=3, 4, 6, 8$. Then $F(a_1)=3, 6$; $f(a_1)=3$, $f(0)=6$; $F(a_2)=4, 6, 8$; $f(a_2)=4, 8$. Thus

$$F(a_1, a_2) - F(a_1) - F(a_2) + F(0) = S - (3, 6) - (4, 6, 8) + 6 \equiv 0 = f(a_1, a_2).$$

A. Berger^{17a} called f_1 conjugate to f_2 if $\sum f_1(d)f_2(d) = 1$ for $k=1$, 0 for $k>1$, when d ranges over the divisors of k . Let $g(mn) = g(m)g(n)$, $g(1)=1$. Write $h(k) = \sum f(d)f_1(\delta)g(\delta)$, where $d\delta=k$. Then $f(k) = \sum f_2(d)g(d)h(\delta)$. Dedekind's inversion formula is a special case. For, if $f_1(n) \equiv 1$, then $f_2(n) \equiv \mu(n)$.

K. Zsigmondy¹⁸ stated that if, for every positive integer r ,

$$\sum_c f(r_c) = F(r),$$

where c ranges over all combinations of powers $\leq r$ of the relatively prime positive integers n_1, \dots, n_p , while r_c denotes the greatest integer $\leq r/c$, then

$$f(r) = F(r) - \sum_n F(r_n) + \sum_{n,n'} F(r_{nn'}) - \dots,$$

where the summation indices n, n', \dots range over the combinations of n_1, \dots, n_p taken 1, 2, \dots at a time.

R. D. von Sterneck¹⁹ noted that, if d ranges over the divisors of n $\sum \theta(d) = \psi(n)$ implies that

$$F(m) \equiv \psi(1) + \dots + \psi(m) = \sum_{j=1}^m \theta(j) \left[\frac{m}{j} \right].$$

Taking $m=1, \dots, n$ and solving, we get $\theta(n)$ expressed as a determinant of order n , whence

$$\theta(n) = \psi(n) - \sum \psi(d_1) + \sum \psi(d_2) - \dots + (-1)^v \psi(d_v),$$

if $n = p_1^{a_1} \dots p_v^{a_v}$ and d_p is derived from n by reducing p exponents by unity.

*Here and in the statement of the theorem occur confusing misprints for k and n .

^{17a}Nova Acta Regiae Soc. Sc. Upsaliensis, (3), 14, 1891, No. 2, 46, 104.

¹⁸Jour. für Math., 111, 1893, 346. Applied in Ch. V, Zsigmondy.⁷⁷

¹⁹Monatshefte Math. Phys., 4, 1893, 53-6.

P. Bachmann²⁰ proved that $f(n) = \sum_{k=1}^{k=\infty} F(kn)$ implies that

$$F(1) = \sum_{n=1}^{\infty} \mu(n)f(n).$$

Write $X = [x/n]$. Taking $F(n) = X$, nX , $\Phi(X)$, whence $f(n) = T(X)$, $n\sigma(X)$, $D(X)$, respectively, we obtain Lipschitz's⁵⁰ (Ch. X) formulas:

$$[x] = \sum_{n=1}^{[x]} \mu(n)T\left[\frac{x}{n}\right] = \sum \mu(n)n\sigma\left[\frac{x}{n}\right], \quad \Phi[x] = \sum \mu(n)D\left[\frac{x}{n}\right].$$

Let $F(n)$ be zero if n is not a divisor of P and write $\psi(P/n)$ for $F(n)$. Hence if d divides P , $f(d) = \sum \psi(P/kd)$ implies $\psi(P) = \sum \mu(d)f(d)$, where k ranges over the divisors of P/d , and d over those of P .

D. von Sterneck²¹ considered a function $f(n)$ with the properties: (i) $f(1) = 1$; (ii) the g. c. d. of $f(m)$ and $f(n)$ is $f(d)$ if d is the g. c. d. of m and n ; (iii) for primes p , other than specified ones, one of the numbers $f(p \pm 1)$ is divisible by p ; (iv) the g. c. d. of $f(\rho n)/f(n)$ and $f(n)$ divides ρ . Then if $L(n)$ is the l. c. m. of the values of f for all the divisors $< n$ of n , $F(n) = f(n) \div L(n)$ is an integer which can be given the form

$$F(n) = \frac{f(n)\Pi f\left(\frac{n}{p_i p_j}\right)\Pi f\left(\frac{n}{p_i p_j p_k p_l}\right) \dots}{\Pi f\left(\frac{n}{p_i}\right)\Pi f\left(\frac{n}{p_i p_j p_k}\right) \dots}, \quad n = \Pi p_i^{l_i}.$$

The four properties hold for the function defined by the recursion formula $f(n) = \alpha f(n-1) + \beta f(n-2)$, where α and β are relatively prime, with the initial conditions $f(1) = 1$, $f(2) = \alpha$. For $\alpha = 2x$, $\beta = b - x^2$, we have²²

$$f(n) = \frac{(x + \sqrt{b})^n - (x - \sqrt{b})^n}{2\sqrt{b}}.$$

The case $\alpha = \beta = 1$ was discussed by Lucas²³ of Ch. XVII, and his test for primality holds for the present generalization.

The four properties hold also for

$$f(n) = \frac{a^n - b^n}{a - b},$$

if a, b are relatively prime;²³ then $f(p-1)$ is divisible by p if p is a prime not dividing a, b or $a-b$.

K. Zsigmondy²⁴ gave a generalized inversion formula. Let N be any multiple of the relatively prime integers n_1, \dots, n_s . Set

$$F(m, N, \epsilon) = \sum f\left(\left[\frac{m}{d}\right], \frac{N}{d}, \epsilon d\right),$$

where d ranges over those divisors $\leq m$ of N which are products of powers

²⁰Die Analytische Zahlentheorie, 1894, 310.

²¹Monatshefte Math. Phys., 7, 1896, 37, 342.

²²Dirichlet, Werke, 1, 47-62. See Dirichlet,⁹ Ch. XVII.

²³Zsigmondy, Monatshefte Math. Phys., 3, 1892, 265.

²⁴Ibid., 7, 1896, 190-3.

of n_1, \dots, n_s . Then, if a ranges over those divisors d which are divisible by no one of $\nu_1, \dots, \nu_{s'}$, chosen from n_1, \dots, n_s ,

$$\sum_a f\left(\left[\frac{m}{a}\right], \frac{N}{a}, \epsilon a\right) = F(m, N, \epsilon) - \sum_{\nu'} F\left(\left[\frac{m}{\nu}\right], \frac{N}{\nu}, \epsilon \nu\right) \\ + \sum_{\nu, \nu'} F\left(\left[\frac{m}{\nu \nu'}\right], \frac{N}{\nu \nu'}, \epsilon \nu \nu'\right) - \dots$$

The left member equals $F(m, N, \epsilon)$ constructed for the numbers other than $\nu_1, \dots, \nu_{s'}$ of the set n_1, \dots, n_s . For $s' = s$, we have

$$f(m, N, \epsilon) = F(m, N, \epsilon) - \sum_n F\left(\left[\frac{m}{n}\right], \frac{N}{n}, \epsilon n\right) + \dots$$

The latter becomes the series in Bachmann²⁰ when $m = \infty$, $N = 0$, $\epsilon = 1$, while n_1, n_2, \dots are primes.

F. Mertens²⁵ considered $\sigma(n) = \mu(1) + \mu(2) + \dots + \mu(n)$ and proved that

$$\sum_{j=g+1}^n \mu(j) \left[\frac{n}{j}\right] = \sigma\left(\frac{n}{1}\right) + \sigma\left(\frac{n}{2}\right) + \dots + \sigma\left(\frac{n}{g}\right) - g\sigma(g), \\ \sigma(n) = 2\sigma(g) - \sum_{r,s=1}^g \mu(r)\mu(s) \left[\frac{n}{rs}\right], \quad g = [\sqrt{n}].$$

By means of a table (pp. 781–830) of the values of $\sigma(n)$ and $\mu(n)$ for $n < 10000$, it is verified that $|\sigma(n)| < \sqrt{n}$ for $1 < n < 10000$.

D. von Sterneck²⁶ verified the last result up to 500 000, and for 16 larger values under 5 million.

A. Berger²⁷ noted that, if $g(m)g(n) = g(mn)$, $g(1) = 1$,

$$\sum \mu(d)g(d) = \prod \{1 - g(p)\} \quad (n > 1),$$

where d ranges over all divisors of n , p over the prime divisors of n . If $\sum g(m)$ is absolutely convergent,

$$\sum_{k=1}^{\infty} \mu(k)g(k) = \prod \{1 - g(p)\},$$

where p ranges over all primes.

D. von Sterneck²⁸ noted that, if $\theta(x) \leq 1$ for every x and if

$$\sum_{x=1}^n \theta(x) \left[\frac{n}{x}\right] = f(n),$$

then

$$\left| \sum_{k=1}^n \theta(k) \right| < \frac{n}{9} + 6 + \left| f(n) - f\left[\frac{n}{2}\right] - f\left[\frac{n}{3}\right] - f\left[\frac{n}{6}\right] \right|.$$

In particular, $|\sum \mu(k)| < 8 + n/9$.

D. F. Seliwanov²⁹ gave Dedekind's formula with application to $\phi(n)$.

H. von Koch^{29a} defined $\mu(k)$ by use of infinite determinants.

²⁵Sitzungsber. Ak. Wiss. Wien (Math.), 106, IIa, 1897, 761–830.

²⁶*Ibid.*, 835–1024; 110, IIa, 1901, 1053–1102; 121, IIa, 1912, 1083–96; Proc. Fifth Intern. Congress Math., 1912, I, 341–3.

²⁷Öfversigt Vetenskaps-Akad. Förhand., Stockholm, 55, 1898, 579–618.

²⁸Monatshefte Math. Phys., 9, 1898, 43–5.

²⁹Math. Soc. St. Pétersbourg, 1899, 120.

^{29a}Öfversigt K. Vetensk.-Akad. Förhand., Stockholm, 57, 1900, 659–68.

E. B. Elliott⁹⁶ of Ch. V gave a generalization of $\mu(n)$.

L. Kronecker³⁰ defined the function $\rho(n, k)$ of the g. c. d. (n, k) of n, k to be 1 if $(n, k) = 1$, 0 if $(n, k) > 1$, and proved for any function $f(n, k)$ of (n, k) the identity

$$\sum_{k=1}^n \rho(n, k) f(n, k) = \sum_d \sum_{k=1}^{n/d} \mu(d) f(n, kd),$$

where d ranges over the divisors of n . The left member is thus the sum of the values of $f(n, k)$ for $k < n$ and prime to n . Set

$$F(n, d) = \sum_{k=1}^{n/d} f(n, kd), \quad \Phi(n, d) = \sum_{k=1}^{n/d} \rho\left(\frac{n}{d}, k\right) f(n, kd).$$

Thus when d ranges over the divisors of n ,

$$F(n, 1) = \sum_d \Phi(n, d), \quad \Phi(n, 1) = \sum_d \mu(d) F(n, d)$$

are consequences of each other. The same is true (p. 274) for

$$h(n) = \sum f(d) g\left(\frac{n}{d}\right), \quad f(n) = \sum \mu(d) g(d) h\left(\frac{n}{d}\right),$$

if $g(rs) = g(r)g(s)$. Application is made (p. 335) to mean values.

E. M. L  meray³¹ gave a generalized inversion theorem. Let $\psi_2(a, b)$ be symmetrical in a, b and such that the function ψ_3 defined by

$$\psi_3(a, b, c) = \psi_2\{a, \psi_2(b, c)\}$$

is symmetrical in a, b, c . Then the function

$$\psi_4(a, b, c, d) = \psi_3\{a, b, \psi_2(c, d)\}$$

will be symmetrical in a, b, c, d and similarly for $\psi_k(a_1, \dots, a_k)$. For example,

$$\psi_2(a, b) = a\sqrt{1+b^2} + b\sqrt{1+a^2}, \quad \psi_3 = abc + \Sigma a\sqrt{1+b^2}\sqrt{1+c^2}.$$

Let $v = \Omega(y, u)$ be the solution of $y = \psi_2(u, v)$ for v . The theorem states that, if d_1, \dots, d_k are the divisors of $m = p^\alpha q^\beta r^\gamma \dots$ and if $F(m)$ be defined by

$$F(m) = \psi_k\{f(d_1), \dots, f(d_k)\},$$

we have inversely $f(m) = \Omega(G, H)$, where

$$G = \psi_\mu \left\{ F(m), F\left(\frac{m}{pq}\right), F\left(\frac{m}{pr}\right), \dots, F\left(\frac{m}{pqrs}\right), \dots \right\},$$

$$H = \psi_\nu \left\{ F\left(\frac{m}{p}\right), F\left(\frac{m}{q}\right), \dots, F\left(\frac{m}{pqr}\right), \dots \right\},$$

where μ is the number of combinations of the distinct prime factors p, q, \dots of m taken 0, 2, 4, \dots at a time, and ν the number taken 1, 3, 5, \dots at a time.

L. Gegenbauer³² defined $\mu(x)$ to be +1 if x is a unit of the field $R(i)$ of complex integers or a product of an even number of distinct primes of

⁹⁶Vorlesungen   ber Zahlentheorie, I, 1901, 246-257. His ϵ_n is $\mu(n)$.

³¹Nouv. Ann. Math., (4), 1, 1901, 163-7.

³²Verslag. Wiss. Ak. Wetenschappen, Amsterdam, 10, 1901-2, 195-207 (German.) English transl. in Proc. Sect. Sc. Ak. Wet., 4, 1902, 169-181.

$R(i)$, -1 if a product of an odd number, 0 if x is divisible by the square of a prime of $R(i)$. Let $\{m\}$ denote a complete set of residues $\neq 0$ of complex integers modulo m . Then the sum of the values of $f(x)$ for all complex integers x relatively prime to a given one n , which are in $\{m\}$, equals $\Sigma \mu(d) \Sigma f(dx)$, where d ranges over all divisors of n in $\{m\}$, and x ranges over $\{m/d\}$. This is due, for the case of real numbers, to Nazimov¹⁶⁷ of Chapter V. Again, $\Sigma \mu(d) = 1$ or 0 according as norm n is 1 or > 1 . Also $\Sigma f(d) = F(n)$ implies $\Sigma \mu(d) F(n/d) = f(n)$.

J. C. Kluyver³³ employed Kronecker's³⁰ identity for special functions f and obtained known results like

$$\Sigma \cos \frac{2\pi \nu}{n} = \mu(n), \quad \Pi 2 \sin \frac{\pi \nu}{n} = e^{\gamma(n)},$$

where ν ranges over the integers $< n$ and prime to n , while $\gamma(n)$ is Bougaief's¹⁶ function $\nu(n)$.

P. Fatou³⁴ noted that Merten's $\sigma(n)$ does not oscillate between finite limits. E. Landau³⁵ proved that it is at most of the order of ne^t , where $t = -a\sqrt{\log n}$. Landau³⁶ noted that Furlan³⁷ made a false use of analysis and ideal theory to obtain a result of Landau's on Merten's²⁵ $\sigma(n)$.

O. Meissner^{37a} employed primes p_i, q_i . For $n = \Pi p_i^{e_i}$ set $Z(n) = \Pi e_i^{p_i}$ and $Z_2(n) = Z\{Z(n)\}$. Then $Z(n) = n$ only if n is $\Pi p_i^{p_i}$ or 16 or $\Pi p_i^{q_i p_i}$. Next, $Z_2(n) = n$ in these three cases and when the exponents e_i in n are distinct primes; otherwise, $Z_2(n) < n$. We have $[1/Z(n)] = \mu^2(n)$.

R. Hackel³⁸ extended the method of von Sterneck²⁸ and obtained various closer approximations, one³⁹ being

$$\left| \Sigma \theta(k) \right| < \frac{n}{26} + 152 + \left| \Sigma f\left[\frac{n}{a}\right] - \Sigma f\left[\frac{n}{b}\right] \right|,$$

where $a = 1, 6, 10, 14, 105$; $b = 2, 3, 5, 7, 11, 13, 385, 1001$.

W. Kusnetzov⁴⁰ gave an analytic expression for $\mu(n)$.

K. Knopp¹⁶⁰ of Ch. X gave many formulas involving $\mu(n)$.

A. Fleck^{40a} generalized $\mu(m) \equiv \mu_1(m)$ by setting

$$\mu_k(m) = \prod_{i=1}^{\lambda} (-1)^{a_i} \binom{k}{a_i}, \quad m = \prod_{i=1}^{\lambda} p_i^{a_i}.$$

Using the zeta function (12) of Ch. X, and ϕ_k of Fleck¹²⁵ of Ch. V, we have

$$\sum_{d|m} \mu_k(d) = \mu_{k-1}(m), \quad \sum_{m=1}^{\infty} \frac{\mu_{k-1}(m)}{m^s} = \zeta(s) \sum_{m=1}^{\infty} \frac{\mu_k(m)}{m^s}, \quad \phi_k(m) = \sum_{d|m} d \mu_{k+1}\left(\frac{m}{d}\right).$$

³³Verslag. Wiss. Ak. Wetenschappen, Amsterdam, 15, 1906, 423-9. Proc. Sect. Sc. Ak. Wet., 9, 1906, 408-14.

³⁴Acta Math., 30, 1906, 392.

³⁵Rend. Circ. Mat. Palermo, 26, 1908, 250.

³⁶Rend. Circ. Mat. Palermo, 23, 1907, 367-373.

³⁷Monatshefte Math. Phys., 18, 1907, 235-240.

^{37a}Math. Naturw. Blätter, 4, 1907, 85-6.

³⁸Sitzungsber. Ak. Wiss. Wien (Math.), 118, 1909, IIa, 1019-34.

³⁹Sylvester, Messenger Math., (2), 21, 1891-2, 113-120.

⁴⁰Mat. Sbornik (Math. Soc. Moscow), 27, 1910, 335-9.

^{40a}Sitzungsber. Berlin Math. Gesell., 15, 1915, 3-8.

The theorem $\sum_{n=1}^{\infty} \mu(n)/n = 0$ and other results on sums involving $\mu(n)$ play an important rôle in the theory of the asymptotic distribution of primes. In accord with the plan of not entering into details on that topic (Ch. XVIII), the reader is referred for the former topic to the history and exposition by E. Landau,⁴¹ and to the subsequent papers by A. Axer,⁴² E. Landau,⁴³ and J. F. Steffensen.⁴⁴

Proofs of (2) or (3) are given in the following texts:

- P. Bachmann, *Die Lehre von der Kreistheilung*, 1872, 8–11; *Die Elemente der Zahlentheorie*, 1892, 40–4; *Grundlehren der Neueren Zahlentheorie*, 1907, 26–9.
 T. J. Stieltjes, *Théorie des nombres*, Ann. fac. Toulouse, 4, 1890, 21.
 Borel and Drach, *Introd. théorie des nombres*, 1895, 24–6.
 E. Cahen, *Éléments de la théorie des nombres*, 1900, 346–350.
 E. Landau,⁴¹ 577–9.

NUMERICAL INTEGRALS AND DERIVATIVES.

N. V. Bougaief⁵⁵ (Bugaiiev) called $F(n)$ the numerical integral of $f(n)$ if $F(m) = \sum f(\delta)$, summed for all the divisors δ of m , and called $f(n)$ the numerical derivative function of $F(n)$, denoted by $DF(n)$ symbolically.

Granting that there is, for every n , the development

$$F(n) = a_1[n] + a_2\left[\frac{n}{2}\right] + a_3\left[\frac{n}{3}\right] + \dots$$

where $[x]$ is the largest integer $\leq x$, then a_k is the numerical derivative of $F(k) - F(k-1)$. He developed $[n^{1/2}]$, $[n^{1/3}]$, etc.

N. V. Bougaief,⁵⁶ after amplifying the preceding remarks, proved that

$$\sum_{d\delta=n} \theta(\delta) \chi(d) = \psi(n), \quad \theta(n) \theta(m) = \theta(nm)$$

imply

$$\chi(n) = \theta(n) D \left\{ \frac{\psi(n)}{\theta(n)} \right\}.$$

Writing $D^{-1}\theta(d)$ for $\sum \theta(d)$, summed for the divisors d of n , we have

$$D^\mu \sum \chi(\delta) \theta(d) = \sum \chi(\delta) D^\mu \theta(d),$$

for any integer μ , positive or negative. There are formulas like

⁴¹Handbuch... Verteilung der Primzahlen, II, 1909, 567–637, 676–96, 901–2.

⁴²Prace mat. fiz., Warsaw, 21, 1910, 65–95; Sitzungsber. Ak. Wiss. Wien (Math.), 120, 1911, IIa, 1253–98.

⁴³Sitzungsber. Ak. Wiss. Wien. (Math.), 120, 1911, IIa, 973–88; Rend. Circ. Mat. Palermo, 34, 1912, 121–31.

⁴⁴Analytiske Studier... Diss., Kjobenhavn, 1912, 148 pp. Fortschritte, 43, 262–3. Extract in Acta Math., 37, 1914, 75–112.

⁵⁵Journal de la Soc. Philomatique de Moscou, 5, 1871.

⁵⁶Theory of numerical derivatives, Moscow, 1870–3, 222 pp. Extracts from Mat. Sbornik (Math. Soc. Moscow), 5, I, 1870–2, 1–63; 6, 1872–3, I, 133–180, 199–254, 309–360 (reviewed in Bull. Sc. Math. Astr., 3, 1872, 200–2; 5, 1873, 296–8; 6, 1874, 314–6). Résumé by Bougaief, Bull. Sc. Math. Astr., 10, I, 1876, 13–32.

$$n = \sum_{u=1}^n \mu^2(u) [\sqrt{n/u}], \quad \sum_{u=1}^n \phi(u) = \frac{1}{2} + \frac{1}{2} \sum \mu(u) \left[\frac{n}{u} \right]^2,$$

$$\Sigma \theta \left(\frac{n}{a} \right) \equiv \theta(\sqrt{n}) \pmod{2}, \quad \Sigma \theta \left(\frac{n}{a^2} \right) - \Sigma \theta \left(\frac{n}{ab} \right) \equiv \theta(\sqrt[3]{n}) \pmod{3},$$

where $\theta(n)$ is the number of primes $a \leq n$. Other special results were cited under 155, Ch. V; 6, Ch. XI; 217, Ch. XVIII.

E. Cesàro^{56a} treated $\Sigma f(\delta)$ in connection with median and asymptotic formulas.

Bougaief⁵⁷ treated numerical integrals, noting formulas like

$$\Sigma_{d|n} \xi \left(\frac{n}{d} \right) \psi(d) = \Sigma_{d|n} \psi(d) + \Sigma_{d|n} \psi(d) + \dots,$$

where $\xi(n)$ is the number of prime factors a, b, \dots of $n = a^a b^b \dots$,

$$\Sigma_{d|n} \psi(d) = \Sigma_{d|n} \psi(d) + \Sigma_{d|n} \psi(a^a d) = \Sigma_{d|n} \psi(ad) + \Sigma_{d|n} \psi(d).$$

Bougaief⁵⁸ gave a large number of formulas of the type

$$\Sigma \psi(d) \left[\frac{n}{d} \right] = \Sigma^n \psi(d) + \Sigma^{[n/2]} \psi(d) + \Sigma^{[n/3]} \psi(d) + \dots,$$

where, on the left, d ranges over all the divisors of m ; while, on the right, d ranges over those divisors of m which do not exceed $n, [n/2], \dots$, respectively.

Bougaief⁵⁹ gave the relation

$$\Sigma_{d|n} \theta(\sqrt{d}) = \Sigma_p \xi_0 \left(\frac{n}{p^2}, n \right),$$

where p ranges over all primes $\leq \sqrt{n}$, and $\xi_k(m, n)$ is the sum of the k th powers of all divisors $\leq m$ of n , so that ξ_0 is their number, and $\theta(t)$ is the number of primes $\leq t$.

L. Gegenbauer⁶⁰ noted that the preceding result is a case of

$$\Sigma_{d|n} g(d) h \left(\frac{n}{d} \right) \Sigma_{\lambda=1}^d f(\lambda) = \Sigma_{\lambda=1}^n f(\lambda) \left\{ \Sigma_{d_\lambda} g(d_\lambda) h \left(\frac{n}{d_\lambda} \right) \right\},$$

where d_λ ranges over the divisors $\geq \lambda$ of n . Special cases are

$$\Sigma_d d^p \theta_k \left(d^{\frac{1}{\mu}} \right) = \Sigma_a a^k \bar{\xi}_p(a^\mu, n), \quad \Sigma_d d^p \theta_k \left\{ \left(\frac{n}{d} \right)^{\frac{1}{\mu}} \right\} = \Sigma_a a^k \xi_p \left(\frac{n}{a^\mu}, n \right),$$

where $\bar{\xi}_p(m, n)$ is the sum of the p th powers of the divisors $\geq m$ of n .

^{56a}Giornale di Mat., 25, 1887, 1-13.

⁵⁷Mat. Sbornik (Math. Soc. Moscow), 14, 1888-90, 169-197; 16, 1891, 169-197 (Russian).

⁵⁸*Ibid.*, 17, 1893-5, 720-59.

⁵⁹Comptes Rendus Paris, 119, 1894, 1259.

⁶⁰Monatshefte Math. Phys., 6, 1895, 208.

Bougaief^{60a} noted that, for an arbitrary function ψ ,

$$\Sigma \psi(d) \left[\frac{n^2+a}{d} \right] = \sum_{u=1}^n \sum_{n=1}^{[(n^2+a)/u]} \psi(d), \quad \sum_{u=1}^n \sum_{n=1}^{[n^2/u]} \psi(d) = n \sum_{u=1}^n \sum_{n=1}^{[n/u]} \psi(d).$$

N. V. Bervi⁶¹ treated numerical integrals extended over solutions of indeterminate equations, in particular for $n = a + b(x+y) + cxy$, $b^2 = b + ac$.

Bougaief⁶² considered definite numerical integrals, viz., sums over all divisors, between a and b , of n . He expressed sums of $[x]$, the greatest integer $\leq x$, as sums of values of $\zeta(n, m)$, viz., the number of divisors $\leq n$ of m . Also sums of ζ 's expressed as $\zeta_i(1) + \zeta_i(2) + \dots + \zeta_i(n)$, where $\zeta_i(n)$ is the number of the divisors of n which are i th powers.

I. I. Cistiakov^{62a} (Tschistiakow) treated the second numerical derivative.

Bougaief^{62b} gave 13 general formulas on numerical integrals.

Bougaief⁶³ gave a method of transforming a sum taken over $1, 2, \dots, n$ into a sum taken over all the divisors of n . He obtains various identities between functions.

D. J. M. Shelly,⁶⁴ using distinct primes a, b, \dots , called

$$N' = N \left(\frac{a}{a} + \frac{\beta}{b} + \dots \right)$$

the derivative of $N = a^\alpha b^\beta \dots$. Similar definitions are given for derivatives of fractions and for the case of fractional exponents α, β, \dots . The primes are the only integers whose derivatives are unity.

^{60a}Comptes Rendus Paris, 120, 1895, 432-4.

⁶¹Mat. Sbornik (Math. Soc. Moscow), 18, 1896, 519; 19, 1897, 182.

⁶²*Ibid.*, 18, 1896, 1-54 (Russian); see Jahrb. Fortschritte Math., 27, 1896, p. 158.

^{62a}*Ibid.*, 20, 1899, 595; see Fortschritte, 1899, 194.

^{62b}*Ibid.*, 549-595. Two of the formulas are given in Fortschritte, 1899, 194.

⁶³*Ibid.*, 21, 1900, 335, 499; see Fortschritte, 31, 1900, 197.

⁶⁴Asociación española, Granada, 1911, 1-12.

CHAPTER XX.

PROPERTIES OF THE DIGITS OF NUMBERS.

John Hill¹ noted that $139854276 = 11826^2$ is formed of the nine digits permuted and believed erroneously that it is the only such square.

N. Brownell^{1a} found 169 and 961 as the squares whose three digits are in reverse order and whose roots are composed of the same digits in reverse order. The least digit in the roots is also the least in the squares, while the greatest digit in the roots is one-third of the greatest in the squares and one-half of the digit in the tens place.

W. Saint^{1b} proved that every odd number N not divisible by 5 is a divisor of a number $11\dots 1$ of $D \leq N$ digits [by a proof holding only for N prime also to 3]. For, let $1\dots 1$ (to D digits) have the quotient q and remainder r when divided by D . This remainder r must recur if the number of digits 1 be increased sufficiently. Hence let $1\dots 1$ (to $D+d$ digits) give the remainder r and quotient Q when divided by D . By subtraction, $D(Q-q) = 1\dots 10\dots 0$ (with d units followed by D zeros). Hence if $1\dots 1$ (to d digits) were not divisible by every odd number $\leq D$ and prime to 5 [and to 3], there would be a remainder R ; then $R0\dots 0$ (with D zeros) would be divisible by an odd number prime to 5 [and to 3], which is impossible.

P. Barlow^{1c} stated, and several gave inadequate proofs, that no square has all its digits alike. He^{1d} stated and proved that $11111111^2 = 12345678987654321$ is the largest square such that if unity be subtracted from each of its digits and again from each digit of the remainder, etc., all zeros being suppressed, each remainder is a square. Denote $(10^k - 1)/(10 - 1)$ by $\{k\}$. Then $\{\frac{1}{2}(x+1)\}^2$ has x digits and exceeds $\{x\}$ by $10\{\frac{1}{2}(x-1)\}^2$. Since zeros are suppressed we have a square as remainder, and the process can be repeated. It is stated that therefore the property holds only for 1^2 , 11^2 , 111^2 ,

Several^{1e} found that 135 is the only number N composed of three digits in arithmetical progression such that the digits will be reversed if 132 times the middle digit be added to N .

W. Saint^{1f} found the least integral square ending with the greatest number of equal digits. The possible final digits are 1, 4, 5, 6, 9. Any square is of the form $4n$ or $4n+1$. Hence the final digit is 4. If the square terminated with more than three 4's, its quotient by 4 would be a square ending with two 1's, just proved to be impossible. Of the numbers ending with

¹Arithmetic, both in Theory and Practice, ed. 4, London, 1727, 322.

^{1a}The Gentleman's Diary, or Math. Repository, London, 1767; Davis' ed., 2, 1814, 123.

^{1b}Jour. Nat. Phil. Chem. Arts (ed., Nicholson), London, 24, 1809, 124-6.

^{1c}The Gentleman's Diary, or Math. Repository, London, 1810, 38-9, Quest. 952.

^{1d}*Ibid.*, 1810, 39-40, Quæst. 953.

^{1e}*Ibid.*, 1811, 33-4, Quest. 960.

^{1f}Ladies' Diary, 1810-11, Quest., 1218; Leybourn's M. Quest. L. D., 4, 1817, 139-41.

three 4's, the least is 1444. J. Davey discussed only numbers of 3 or 4 digits of which the last 2 or 3 are equal, respectively.

Several¹⁹ found that the squares 169 and 961 are composed of the same digits in reverse order, have roots of two digits in reverse order, while the sum of the digits in each square equals the square of the sum of the digits in each root; finally, the sum of the digits in each root equals the square of their difference.

An anonymous writer² proposed the problem to find a number n given the product of n by the number obtained from n by writing its digits in reverse order [Laisant¹⁸].

P. Tédénat³ considered the problem to find a number of n digits whose square ends with the same n digits in the same order. If a is such a number of $n-1$ digits, so that $a^2 = 10^{n-1}b + a$, we can find a digit A to annex at the left of a to obtain a desired number $10^{n-1}A + a$ of n digits. Squaring the latter, we obtain the condition $(2a-1)A \equiv -b \pmod{10}$.

J. F. Français⁴ noted the solutions

$$\begin{aligned} x &= 2^n p = 5^n q + 1, & x^2 &= 10^n pq + x, \\ y &= 5^n r = 2^n s + 1, & y^2 &= 10^n rs + y, \end{aligned}$$

in which the resulting condition $2^n p - 5^n q = 1$ or $5^n r - 2^n s = 1$ is to be satisfied. Special solutions are given by $n=1$, $p=3$; $n=2$, $p=19$; $n=3$, $p=47$; $n=4$, $p=586$; etc., to $n=7$.

J. D. Gergonne⁵ generalized the problem to base B . Then

$$x(x-1) = B^n y.$$

Let p, q be relatively prime and set $B^n = pq$. Then $x = pt$, $x-1 = qu$, or vice versa. The condition $pt - qu = 1$ is solved for t, u . When $B=10$, $n=20$, the least u is 81199.

Anonymous writers⁶ stated and proved by use of the decimal fraction for $1/n$ that every number divides a number of the form $9 \dots 90 \dots 0$.

A. L. Crelle⁷ proved the generalization: Every number divides a number obtained by repeating any given set of digits and affixing a certain number of zeros, as $23 \dots 230 \dots 0$.

Several^{7a} found a square whose root has two digits, their quotient being equal to their difference. By $x/y = x-y$, $x = y+1+1/(y-1)$, an integer, whence $y=2$, $x=4$. Thus the squares are 24^2 or 42^2 .

The^{7b} three digits of a number are in geometrical progression; the product of the sum of their cubes by the cube of their sum is 1663129; if the number obtained by reversing the digit be divided by the middle digit, the

¹⁹Ladies' Diary, 1811-12, Quest. 1231; Leybourn, *l. c.*, 153-4.

²Annales de Math. (ed., Gergonne), 3, 1812-3, 384.

³*Ibid.*, 5, 1814-5, 309-321. Problem proposed on p. 220.

⁴*Ibid.*, 321-2.

⁵*Ibid.*, 322-7.

⁶*Ibid.*, 19, 1828-9, 256; 20, 1829-30, 304-5.

⁷*Ibid.*, 20, 1829-30, 349-352; Jour. für Math., 5, 1830, 296.

^{7a}Ladies' Diary, 1820, 36, Quest. 1347.

^{7b}*Ibid.*, 1822, 33, Quest. 1374.

quotient is $46\frac{1}{3}$. By the last condition, the middle digit must be 3, since not a higher multiple of 3. Hence the number is 931.

To find a symmetrical number $abcba$ of five digits whose square exhibits all ten digits, W. Rutherford^{7c} noted that the square is divisible by 9 since the sum of the digits is divisible by 9. Hence the sum of the digits of the number is divisible by 3. Also $a \geq 3$. Taking $c = a + b$, $c = 8$, he got 35853. J. Sampson noted also the answers 84648, 97779.

J. A. Grunert⁸ proved by use of Euler's generalization of Fermat's theorem that⁶ every number divides $9 \dots 90 \dots 0$.

Drot^{8a} asked for the values of x for which N^x has the same final k digits as N , when $k = 1, 2$ or 3 .

J. Bertrand^{8b} discussed the numbers of digits of certain numbers.

A. G. Emsmann⁹ treated a number b of n digits to base 10 equal to the product of the sum of its digits by a , and such that if another number of n digits be subtracted from b the remainder shall equal the number obtained by writing the digits of b in reverse order.

J. Booth¹⁰ noted that a number of six digits formed by repeating any set of three digits is divisible by 7, 11, 13 [since by 1001].

G. Bianchi^{10a} noted various numerical relations like $10^9 = 11111111 + 8.1111111 + 8.9.111111 + \dots + 8.9^6.1 + 9^8 = 2222222 + \dots + 7.8^6.2 + 8^8$, $98 = (12 - 1 - 0)9 - 1$, $987 = (123 - 12 - 1)9 - 3$, $9876 = (1234 - 123 - 13)9 - 6$.

C. M. Ingleby¹¹ added the digits of a number N written to base r , then added the digits of this sum, etc., finally obtaining a number, designated SN , of a single digit; and proved that $S(MN) = S(SM \cdot SN)$.

P. W. Flood^{11a} proved that 64 is the only square the sum of whose digits less unity and product plus unity are squares.

G. Cantor¹² employed any distinct positive integers a, b, \dots , considered the system of integers in which a occurs \bar{a} times, b occurs \bar{b} times, etc., and called a system simple if every number can be expressed in a single way in the form $\alpha a + \beta b + \dots$, where $\alpha = 0, 1, \dots, \bar{a}$; $\beta = 0, 1, \dots, \bar{b}$; A system is simple if and only if each basal number k divides the next one l and if k occurs $\bar{k} = (l/k) - 1$ times.

G. Barillari¹³ noted that, if 10 belongs to the exponent m modulo b , the number $P = \alpha\beta \dots \lambda\alpha\beta \dots \lambda \dots$, obtained by repeating h times ($h > 1$) any set of n digits, is divisible by b if b is prime to $10^n - 1$ and if nh is a multiple

^{7c}Ladies' Diary, 1835, 38, Quest. 1576.

⁸Jour. für Math., 5, 1830, 185-6.

^{8a}Nouv. Ann. Math., 4 1845, 637-44; 5, 1846, 25. For references to tables of powers, 13, 1854, 424-5.

^{8b}Ibid., 8, 1849, 354.

⁹Abhandlung über eine Aufgabe aus der Zahlentheorie, Progr. Frankfurt, 1850, 36 pp.

¹⁰Proc. Roy. Soc. London, 7, 1854-5, 42-3.

^{10a}Proprieta e rapporti de' numeri interi e composti colle cifre semplici . . . , Modena, 1856. Same in Mem. di Mat. e di Fis. Soc. Ital. Sc., Modena, (2), 1, 1862, 1-36, 207.

¹¹Oxford, Cambr. and Dublin Messenger Math., 3, 1866, 30-31.

^{11a}Math. Quest. Educ. Times, 7, 1867, 30.

¹²Zeitschrift Math. Phys., 14, 1869, 121-8.

¹³Giornale di Mat., 9, 1871, 125-135.

of m , but P is not divisible by b if nh is not a multiple of m . If b divides $10^n - 1$, P is divisible by b when $h = b$, but not divisible by b when h is not a multiple of b .

A. Morel¹⁴ proved that the numbers ending with 12, 38, 62 or 88 are the only ones whose squares end with two equal digits.

H. Hoskins^{14a} found the sum of the 117852 numbers of 7 digits which can be formed with the digits 1, 1, 2, 2, 2, 2, 2, 3, 3, 4, 5, 6, 7.

J. Plateau¹⁵ noted that every odd number not ending with 5 has a multiple of the form $11 \dots 1$ [Saint¹⁵].

P. Mansion¹⁶ proved the theorem of Plateau.

J. W. L. Glaisher¹⁷ deduced Crelle's⁷ theorem from Plateau's.¹⁵

C. A. Laisant¹⁸ treated a problem² on reversing digits.

G. R. Perkins^{18a} and A. Martin¹⁹ stated that all powers of numbers ending with 12890625 end with the same digits.

E. Catalan²⁰ noted that the g. c. d. of two numbers of the form $1 \dots 1$ of n and n' digits is of like form and has Δ digits, where Δ is the g. c. d. of n and n' .

Lloyd Tanner,^{20a} generalizing Martin's¹⁹ question, found how many numbers N of n digits to the base r end with the same digits as their squares, i. e., $N^2 - N = Kr^n$. If r^n is the product of q powers of primes, there are $2^q - 2$ values of N . He^{20b} found numbers M and N with n digits to the base r such that the numbers formed by prefixing M to N and N to M have a given ratio.

J. Plateau²¹ proposed the problem to find two numbers whose product has all its digits alike. Angenot noted that

$$\frac{b^{pq} - 1}{b^p - 1}, \quad \frac{b^p - 1}{b - 1}$$

give a solution for base b . Catalan²¹ noted that Euler's theorem

$$\frac{b^{\varphi(n)} - 1}{b - 1} = nm$$

for n prime to b , furnishes a solution n, m .

Lloyd Tanner²² stated and Laisant proved that 87109376 and 12890625 are the only numbers of 8 digits whose squares end with the same 8 digits.

¹⁴Nouv. Ann. Math., (2), 10, 1871, 44-6, 187-8.

^{14a}Math. Quest. Educ. Times, 15, 1871, 89-91.

¹⁵Bull. Acad. Roy. de Belgique, (2), 16, 1863, 62; 28, 1874, 468-476.

¹⁶Nouv. Corresp. Math., 1, 1874-5, 8-12; Mathesis, 3, 1883, 196-7. Bull. Bibl. Storia Sc. Mat., 10, 1877, 476-7.

¹⁷Messenger Math., 5, 1875-6, 3-5.

¹⁸Mém. soc. sc. phys. et nat. de Bordeaux, (2), 1, 1876, 403-11.

^{18a}Math. Miscellany, Flushing, N. Y., 2, 1839, 92.

¹⁹Math. Quest. Educat. Times, 26, 1876, 28.

²⁰Mém. Société Sc. Liège, (2), 6, 1877, No. 4.

^{20a}Messenger Math., 7, 1877-8, 63-4. Cases $r \leq 12$, Math. Quest. Educ. Times, 28, 1878, 32-4.

^{20b}Math. Quest. Educ. Times, 29, 1878, 94-5.

²¹Nouv. Corresp. Math., 4, 1878, 61-63.

²²Ibid., 5, 1879, 217; 6, 1880, 43.

Moret-Blanc²³ proved that 1, 8, 17, 18, 26, 27 are the only numbers equal to the sum of the digits of their cubes.

C. Berdellé^{23a} considered the last n digits of numbers, in particular of 5^k .

E. Cesàro²⁴ noted that the sum of the p th powers of ten consecutive integers ends with 5 unless p is a multiple of 4, when it ends with 3.

F. de Rocquigny²⁵ noted that if a number of n digits equals the sum of the $2^n - 1$ products of its digits taken 1, 2, ..., n at a time, its final $n - 1$ digits are all 9.

E. Cesàro²⁶ considered the period of the digits of rank n in powers of 5.

Lists^{26a} have been given of squares formed by the nine digits > 0 , or the ten digits, not repeated.

O. Kessler²⁷ gave a table of divisors of numbers formed by repeating a given set of digits a small number of times.

T. C. Simmons^{27a} noted that, if the sum of the digits of n is 10, that of $2n$ is 11 unless each digit of n is < 5 or two are 5. For 4 digits the numbers of each type are counted.

J. S. Mackay²⁸ treated the last subject.

E. Lemoine²⁹ considered numbers like $A = 8607004053$ such that, if a is the number derived by reversing the digits of A , the sum $A + a = 12111011121$ reverses into itself.

M. d'Ocagne³⁰ considered the sum $\sigma(N)$ of the digits of the first N integers. If $N_p = a_p \cdot 10^p + \dots + a_1 \cdot 10 + a_0$ and $d = a_p \cdot 10^p - 1$, then

$$\sigma(d) = 10^{p-1} \cdot 5a_p(a_p - 1 + 9p), \quad \sigma(N_p) = \sigma(d) + (N_{p-1} + 1)a_p + \sigma(N_{p-1}).$$

Hence

$$\sigma(N_p) = \frac{1}{2}a_0(a_0 + 1) + \sum_{i=1}^p a_i \{10^{i-1} \cdot 5(a_i - 1 + 9i) + N_{i-1} + 1\}.$$

The number of digits in 1, ..., N is $(p+1)(N+1) - (10^{p+1} - 1)/9$. See the next paper.

M. d'Ocagne³¹ noted that, in writing down the natural numbers 1, ..., N , where N is composed of n digits, the total number of digits written is $n(N+1) - 1_n$, where $1_n = 1 \dots 1$ (to n digits).

E. Barbier^{31a} asked what is the 10^{1000} th digit written if the series of natural numbers be written down.

²³Nouv. Ann. Math., (2), 18, 1879, 329; proposed by Laisant, 17, 1878, 480.

^{23a}Assoc. franç., 8, 1879, 176-9.

²⁴Nouv. Corresp. Math., 6, 1880, 519; Mathesis, 1888, 103.

²⁵Les Mondes, 53, 1880, 410-2.

²⁶Nouv. Corresp. Math., 4, 1878, 387; Nouv. Ann. Math., (3), 2, 1883, 144, 287; 1884, 160.

^{26a}Math. Magazine, 1, 1882-4; 69-70; l'intermédiaire des math., 4, 1897, 168; 14, 1907, 135; Sphinx-Oedipe, 1908-9, 35; 5, 1910, 64; Educ. Times, March, 1905. Math. Quest. Educ. Times, 52, 1890, 61; (2), 8, 1905, 83-6 (with history).

²⁷Zeitschrift Math. Phys., 28, 1883, 60-64.

^{27a}Math. Quest. Educ. Times, 41, 1884, 28-9, 64-5.

²⁸Proc. Edinburgh Math. Soc., 4, 1885-6, 55-56.

²⁹Nouv. Ann. Math., (3), 4, 1885, 150-1.

³⁰Journ. de sc. math. e ast., 7, 1886, 117-128.

³¹Ibid., 8, 1887, 101-3; Comptes Rendus Paris, 106, 1888, 190.

^{31a}Comptes Rendus Paris, 105, 1887, 795, 1238.

L. Gegenbauer^{31b} proved generalizations of Cantor's¹² theorems, allowing negative coefficients. Given the distinct positive integers a_1, a_2, \dots , every positive integer is representable in a single way as a linear homogeneous function of a_1, a_2, \dots with integral coefficients if each a_λ is divisible by $a_{\lambda-1}$ and the quotient equals the number of permissible values of the coefficients of the smaller of the two.

R. S. Aiyar and G. G. Storr^{31c} found the number p_n of integers the sum of whose digits (each >0) is n , by use of $p_n = p_{n-1} + \dots + p_{n-9}$.

E. Strauss³² proved that, if a_1, a_2, \dots are any integers >1 , every positive rational or irrational number <1 can be written in the form

$$\frac{a_1}{a_1} + \frac{a_2}{a_1 a_2} + \frac{a_3}{a_1 a_2 a_3} + \dots \quad (a_1 < a_1, a_2 < a_2, \dots),$$

the a 's being integers, and in a single way except in the case in which all the a_i , beginning with a certain one, have their maximum values, when also a finite representation exists.

E. Lucas³³ noted that the only numbers having the same final ten digits as their squares are those ending with ten zeros, nine zeros followed by 1, 8212890625 and 1787109376. He gave (ex. 4) the possible final nine digits* of numbers whose squares end with 224406889. He gave (p. 45, exs. 2, 3) all the numbers of ten digits to base 6 or 12 whose squares end with the same ten digits. Similar special problems were proposed by Escott and Palmstrom in *l'Intermédiaire des Mathématiciens*, 1896, 1897.

J. Kraus³⁴ discussed the relations between the digits of a number expressed to two different bases.

A. Cunningham^{34a} called N an agreeable number of the m th order and n th degree in the r -ary scale if the m digits at the right of N are the same as the m digits at the right of N^n when each is expressed to base r ; and tabulated all agreeable numbers to the fifth order and in some cases to the tenth. A number N of m digits is completely agreeable if the agreement of N with its n th power extends throughout its m digits, the condition being $N^n \equiv N \pmod{r^m}$.

E. H. Johnson^{34b} noted that, if a and $r-1$ are relatively prime and $aa \dots a$ (to $r-1$ digits to base r) is divided by $r-1$, there appear in the quotient all the digits 1, 2, \dots , $r-1$ except one, which can be found by dividing the sum of its digits by $r-1$.

C. A. Laisant^{34c} stated that, if $N=123 \dots n$, written to base $n+1$, be multiplied by any integer $<n$ and prime to n , the product has the digits of N permuted.

^{31b}Sitzungsber. Ak. Wiss. Wien (Math.), 95, 1887, II, 618-27.

^{31c}Math. Quest. Educ. Times, 47, 1887, 64.

³²Acta Math., 11, 1887-8, 13-18.

³³Théorie des nombres, 1891, p. 38. Cf. Math. Quest. Educ. Times, (2), 6, 1904, 71-2.

*Same by Kraitchik, Sphinx-Oedipe, 6, 1911, 141.

³⁴Zeitschr. Math. Phys., 37, 1892, 321-339; 39, 1894, 11-37.

^{34a}British Assoc. Report, 1893, 699.

^{34b}Annals of Math., 8, 1893-4, 160-2.

^{34c}*L'intermédiaire des math.*, 1894, 236; 1895, 262. Proof by "Nauticus," *Mathesis*, (2), 5, 1895, 37-42.

Tables of primes to the base 2 are cited under Suchanek⁸⁰ of Ch. XIII.

There is a collection^{34d} of eleven problems relating to digits.

To find^{34e} the number < 90 which a person has in mind, ask him to annex a declared digit and to tell the remainder on division by 3, etc.

T. Hayashi³⁵ gave relations between numbers to the base r :

$$123 \dots \{r-1\} \cdot (r-1) + r = 1 \dots 1 \text{ (to } r \text{ digits),}$$

$$\{r-1\} \{r-2\} \dots 321 \cdot (r-1) - 1 = \{r-2\} \{r-2\} \dots \text{ (to } r \text{ digits).}$$

Several writers³⁶ proved that

$$123 \dots \{r-1\} \cdot (r-2) + r - 1 = \{r-1\} \dots 321.$$

T. Hayashi³⁷ noted that if $A = 10 + r(10)^2 + r^2(10)^3 + \dots$ be multiplied or divided by any number, the digits of each period of A are permuted cyclically.

A. L. Andreini^{37a} found pairs of numbers N and p (as 37 and 3) such that the products of N by all multiples $\leq (B-1)p$ of p are composed of p equal digits to the base $B \leq 12$, whose sum equals the multiplier.

P. de Sanctis³⁸ gave theorems on the product of the significant digits of, or the sum of, all numbers of n digits to a general base, or the numbers beginning with given digits or with certain digits fixed, or those of other types.

A. Palmstrom³⁹ treated the problem to find all numbers with the same final n digits as their squares. Two such numbers ending in 5 and 6, respectively, have the sum $10^n + 1$. If the problem is solved for n digits, the $(n+1)$ th digit can be found by recursion formulæ. There is a unique solution if the final digit (0, 1, 5 or 6) is given.

A. Hauke⁴⁰ discussed obscurely $x^m \equiv x \pmod{s^r}$ for x with r digits to base s . If $m=2$, while r and s are arbitrary, there are 2^ν solutions, ν being the number of distinct prime factors of s .

G. Valentin and A. Palmstrom⁴¹ discussed $x^k \equiv x \pmod{10^n}$, for $k=2, 3, 4, 5$.

G. Wertheim⁴² determined the numbers with seven or fewer digits whose squares end with the same digits as the numbers, and treated simple problems about numbers of three digits with prescribed endings when written to two bases.

^{34d}Sammlung der Aufgaben... Zeitschr. Math. Naturw. Unterricht, 1898, 35-6.

^{34e}Math. Quest. Educ. Times, 63, 1895, 92-3.

³⁵Jour. of the Physics School in Tokio, 5, 1896, 153-6, 266-7; Abhand. Geschichte der Math. Wiss., 28, 1910, 18-20.

³⁶Jour. of the Physics School in Tokio, 5, 1896, 82, 99-103; Abhand., 16-18.

³⁷Ibid., 6, 1897, 148-9; Abhand., 21.

^{37a}Periodico di Mat., 14, 1898-9, 243-8.

³⁸Atti Accad. Pont. Nuovi Lincei, 52, 1899, 58-62; 53, 1900, 57-66; 54, 1901, 18-28; Memorie Accad. Pont. Nuovi Lincei, 19, 1902, 283-300; 26, 1908, 97-107; 27, 1909, 9-23; 28, 1910, 17-31.

³⁹Skrifter udgivne af Videnskabs, Kristiania, 1900, No. 3, 16 pp.

⁴⁰Archiv Math. Phys., (2), 17, 1900, 156-9.

⁴¹Forhandlinger Videnskabs, Kristiania, 1900-1, 3-9, 9-13.

⁴²Anfangsgründe der Zahlenlehre, 1902, 151-3.

C. L. Bouton⁴³ discussed the game *nim* by means of congruences between sums of digits of numbers to base 2.

H. Piccioli^{43a} employed $N = a_1 \dots a_n$ of $n \geq 3$ digits and numbers $a_{i_1} \dots a_{i_n}$ and $a_{j_1} \dots a_{j_n}$ obtained from N by an even and odd number of transpositions of digits. Then $\Sigma a_{i_1} \dots a_{i_n} = \Sigma a_{j_1} \dots a_{j_n}$.

If^{43b} a number of n digits to base R has r fixed digits, including the first, and the sum of these r is $\equiv -a \pmod{R-1}$, the number of ways of choosing the remaining digits so that the resulting number shall be divisible by $R-1$ is the number of integers of $n-r$ or fewer digits whose sum is $\equiv a \pmod{R-1}$ and hence is $N+1$ or N , according as $a=0$ or $a>0$, where $N = (R^{n-r} - 1)/(R-1)$.

G. Metcalfe^{43c} noted that 19 and 28 are the only integers which exceed by unity 9 times the integral parts of their cube roots.

A. Tagiuri⁴⁴ proved that every number prime to the base g divides a number $1 \dots 1$ to base g (generalization of Plateau's¹⁵ theorem).

If^{44a} A, B, C have 2, 3, 4 digits respectively and A becomes A' on reversing its digits, and $2A-1=A'$, $3B-2A+10=B'$, $4C-B+1+[B/10]=C'$, then $A=37$, $B=329$, $C=2118$.

P. F. Teilhet⁴⁵ proved that we can form any assigned number of sets, each including any assigned number of consecutive integers, such that with the digits of the q th power of any one of these integers we can form an infinitude of different q th powers, provided $q < m$, where m is any given integer.

L. E. Dickson^{45a} determined all pairs of numbers of five digits such that their ten digits form a permutation of 0, 1, ..., 9 and such that the sum of the two numbers is 93951.

A. Cunningham^{45b} found cases of a number expressible to two bases by a single digit repeated three or more times. He^{45c} noted that all 10 digits or all >0 occur in the square of 101010101010101 or of $1 \dots 1$ (to 9 digits), each square being unaltered on reversing its digits.

He^{45d} and T. Wiggins expressed each integer ≤ 140 by use of four nines, as $13 = 9 + \sqrt{9} + 9/9$, allowing also $.9 = 1$, $(\sqrt{9})!$, and the exponent $\sqrt{9}$, and cited a like table using four fours.

If^{45e} $r \equiv 1 \pmod{q}$, $1 \dots 1$ (with q^n digits to base r) is divisible by q^n .

If^{45f} the square of a number n of r digits ends with those r digits, then $10^r + 1 - n$ has the same property. Also, $(n-1)^3$ ends with the same r digits

⁴³Annals of Math., (2), 3, 1901-2, 35-9. Generalized by E. H. Moore, 11, 1910, 93-4.

^{43a}Nouv. Ann. Math., (4), 2, 1902, 46-7.

^{43b}Math. Quest. Educ. Times, (2), 1, 1902, 119-120.

^{43c}Ibid., 63-4.

⁴⁴Periodico di Mat., 18, 1903, 45.

^{44a}Math. Quest. Educ. Times, (2), 5, 1904, 82-3.

⁴⁵L'intermédiaire des math., 11, 1904, 14-6.

^{45a}Amer. Math. Monthly, 12, 1905, 94-5.

^{45b}Math. Quest. Educ. Times, (2), 8, 1905, 78.

^{45c}Ibid., 10, 1906, 20.

^{45d}Math. Quest. Educ. Times, 7, 1905, 43-46.

^{45e}Ibid., 7, 1905, 49-50.

^{45f}Ibid., 7, 1905, 60-61.

as $n-1$. If the cube of a number n of r digits ends with those r digits, $10^r - n$ has the same property.

P. Zühlke⁴⁶ proved the three theorems of Palmstrom³⁹ and gave all solutions of $x^p \equiv x \pmod{10^3}$ for $p=3, \dots, 12$.

M. Koppe⁴⁷ noted that by prefixing a digit to a solution 0, 1, 5 or 6 of $x^2 \equiv x \pmod{10}$ we get solutions of $x^2 \equiv x \pmod{10^2}$, then for 10^3 , etc. We can pass from a solution with n digits for 10^n to solutions with $2n$ digits for 10^{2n} . He treated also $x^5 \equiv x \pmod{10^n}$.

G. Calvitti⁴⁸ treated the problem: Given a number A , a set C of γ digits, and a number p prime to the base g , to find the least number x of times the set C must be repeated at the right of A to give a number $N_x \equiv A \pmod{p}$. The condition is $G(N_1 - N_0) \equiv 0 \pmod{p}$, where

$$G = \frac{g^{x\gamma} - 1}{g^\gamma - 1}.$$

If $N_1 - N_0 \equiv 0$, any x is a solution. If not, the least value λ of x makes $G \equiv 0 \pmod{p/\rho}$, where ρ is the g. c. d. of $N_1 - N_0$ and p . Then λ is the l. c. m. of $\lambda_1, \dots, \lambda_k$, where λ_i is the least root of $G \equiv 0 \pmod{p_i}$, if p/ρ is the product of p_1, \dots, p_k , relatively prime in pairs. Hence the problem reduces to the case of a power of a prime p . Write $(a)_x$ for $(a^x - 1)/(a - 1)$. It is shown that the least root of $(a)_x \equiv 0 \pmod{p^k}$ is mp^{k-t} , where m is the least root of $(a)_x \equiv 0 \pmod{p}$, and p^t is the highest power of p dividing $(a)_m$. Given any set C of digits and any number p prime to the base g , there exist an infinitude of numbers $C \dots C$ divisible by p .

A. Gérardin^{48a} added 220 to the sum of its digits, repeated the operation 18 times and obtained 418; 9 such operations on 284 gave 418. A. Boutin stated that if a and b lead finally to the same number, neither a nor b is divisible by 3, or both are divisible by 3 and not by 9, or both are divisible by 9.

E. Malo⁴⁹ considered periodicity properties of A and a in

$$5^k = 10^m A_{n,p} + a_p \quad (a_p < 10^m, \quad k = n \cdot 2^{m-2} + p, \quad 0 \leq p \leq 2^{m-2} - 1),$$

and solved Cesàro's²⁶ three problems on the digits of powers of 5.

A. L. Andreini⁵⁰ noted that the squares of A and B end with the same p digits if and only if the smaller of $r+s$ and $u+v$ equals p , where

$$A + B = \alpha \cdot 2^r \cdot 5^u, \quad A - B = \beta \cdot 2^s \cdot 5^v.$$

⁴⁶Sitz. Berlin Math. Gesell., 4, 1905, 10-11 (Suppl., Archiv Math. Phys., (3), 8, 1905).

⁴⁷Ibid., 5, 1906, 74-8. (Suppl., Archiv, (3), 11, 1907.)

⁴⁸Periodico di Mat., 21, 1906, 130-142.

^{48a}Sphinx-Oedipe, 1, 1906, 19, 47-8. Cf. l'interméd. math., 22, 1915, 134, 215.

⁴⁹Sur certaines propriétés arith. du tableau des puissances de 5, Sphinx-Oedipe, 1906-7, 97-107; reprinted, Nancy, 1907, 13 pp., and in Nouv. Ann. Math., (4), 7, 1907, 419-431.

⁵⁰Il Pitagora, Palermo, 14, 1907-8, 39-47.

W. Jänichen^{50b} stated that, if $q_p(x)$ denotes the sum of the digits of x to the base p and if p is a prime divisor of n , then, for μ as in Ch. XIX,

$$\sum_{d|n} \mu(d) q_p\left(\frac{n}{d}\right) = 0.$$

E. N. Barisien^{50c} noted that the sum of all numbers of n digits formed with p distinct digits $\neq 0$, of sum s , is

$$s(p+1)^{n-2} \{p(10^{n-1}-1)/9 + (p+1)10^{n-1}\}.$$

A. Gérardin^{50d} listed all the 124 squares formed of 7 distinct digits.

Several writers⁵¹ treated the problem to find four consecutive numbers $a, b = a+1, c = a+2, d = a+3$, such that $(a)_1 = 11 \dots 1$ (to a digits) is divisible by $a+1$, $(b)_1$ by $2b+1$, $(c)_1$ by $3c+1$, $(d)_1$ by $4d+1$.

A. Cunningham and E. B. Escott⁵² treated the problems to find integers whose squares end with the same n digits or all with n given digits; to find numbers having common factors with the numbers obtained by permuting the digits cyclically, as

$$259 = 7 \cdot 37, \quad 592 = 16 \cdot 37, \quad 925 = 25 \cdot 37.$$

E. N. Barisien⁵³ noted that the squares of 625, 9376, 8212890625 end with the same digits, respectively. R. Vercellin⁵⁴ treated the same topic.

E. Nannei⁵⁵ discussed a problem by E. N. Barisien: Take a number of six digits, reverse the digits and subtract; to the difference add the number with its digits reversed; we obtain one of 13 numbers 0, 9900, ..., 1099989. The problem is to find which numbers of six digits leads to a particular one of these 13, and to generalize to n digits.

Several writers⁵⁶ examined numbers of 6 digits which become divisible by 7 after a suitable permutation of the digits; also⁵⁷ couples of numbers, as 18 and 36, 36 and 54, whose g. c. d. 18 is the sum of their digits.

E. N. Barisien⁵⁸ gave ten squares not changed by reversing the digits, as $676 = 26^2$.

A. Witting⁵⁹ noted that, besides the evident ones 11 and 22, the only numbers of two digits whose squares are derived from the squares of the numbers with the digits interchanged by reversing the digits are 12 and 13. Similarly for the squares of 102 and 201, etc. Also,

$$102 \cdot 402 = 201 \cdot 204, \quad 213 \cdot 936 = 312 \cdot 639, \quad 213 \cdot 624 = 312 \cdot 426.$$

A. Cunningham⁶⁰ treated three numbers L, M, N of l, m, n digits, respectively, such that $N = LM$, and N has all the digits of L and M and no others.

^{50b}Archiv Math. Phys., (3), 13, 1908, 361. Proof by G. Szegő, 24, 1916, 85-6.

^{50c}Sphinx-Oedipe, 1907-8, 84-86. For $p = n$, Math. Quest. Educ. Times, 72, 1900, 126-8.

^{50d}Ibid., 1908-9, 84-5.

⁵¹L'intermédiaire des math., 16, 1909, 219; 17, 1910, 71, 203, 228, 286 [136].

⁵²Math. Quest. Educ. Times, (2), 15, 1909, 27-8, 93-4.

⁵³Suppl. al Periodico di Mat., 13, 1909, 20-21.

⁵⁴Suppl. al Periodico di Mat., 14, 1910-11, 17-20.

⁵⁵Ibid., 13, 1909, 84-88.

⁵⁶L'intermédiaire des math., 17, 1910, 122, 214-6, 233-5.

⁵⁷Ibid., 170, 261-4; 18, 1911, 207.

⁵⁸Mathesis, (3), 10, 1910, 65.

⁵⁹Zeitschrift Math.-Naturw. Unterricht, 41, 1910, 45-50.

⁶⁰Math. Quest. Educ. Times, (2), 18, 1910, 23-24.

D. Biddle⁶¹ applied congruences to find numbers like 15 and 93 whose product 1395 has the same digits as the factors.

P. Cattaneo⁶² considered numbers Q (and C) whose square (cube) ends with the same digits as the number itself. No $Q > 1$ ends with 1. No two Q 's with the same number of digits end with 5 or with 6. All Q 's $< 10^{14}$ are found. A single C of n digits ends with 4 or 6. Any Q is a C . Any $Q-1$ is a C . If N is a Q with n digits and if $2N-1$ has n digits, it is a C .

M. Thié,^{62a} using all nine digits > 0 , found numbers of 2, 3 or 4 digits with properties like $12\cdot483 = 5796$.

Pairs^{62b} of cubes 3^3 , 6^6 and 375^3 , 387^3 whose sums of digits are squares, 3^2 and 6^2 .

T. C. Lewis⁶³ discussed changes in the digits of a number to base r not affecting its divisibility by p .

Numbers⁶⁴ B and B^n having the same sum of digits.

Pairs⁶⁵ of primes like $23\cdot89 = 29\cdot83$.

Cases⁶⁶ like $7\cdot9403 = 65821$ and $3\cdot1458 = 6\cdot0729$, where the digits 0, 1, ..., 9 occur without repetition.

N^{pn+1} ending⁶⁷ with the same digits as N .

Numbers⁶⁸ like $512 = (5+1+2)^3$, $47045881000000 = (47+4+58+81)^6$.

All⁶⁹ numbers like $2\cdot5\cdot27 = 1\cdot18\cdot15$, $2+5+27 = 1+15+18$.

Number⁷⁰ divisible by the same number reversed.

Number⁷¹ an exact power of the sum of its digits; two numbers each an exact power of the sum of the digits of the other.

Solve⁷² $KN+P=N'$, N' derived from N by reversing the digits.

Symmetrical numbers (*ibid.*, p. 195).

F. Stasi⁷³ proved that, if a , b are given integers and a has m digits, we can find a multiple of b of the form

$$10^{\rho}(a\cdot10^{mi} + a\cdot10^{m(i-1)} + \dots + a), \quad \rho \geq 0.$$

Taking b prime to a and to 10, we see that b divides $10^{mi} + \dots + 1$. The case $m=1$ gives the result of Plateau.¹⁵

Cunningham^{73a} and others wrote N_1 for the sum of N and its digits to base r , N_2 for the sum of N_1 and its digits, etc., and found when N_m is divisible by $r-1$.

⁶¹Math. Quest. Educ. Times, (2), 19, 1911, 60-2. Cf. (2), 17, 1900, 44.

⁶²Periodico di Mat., 26, 1911, 203-7.

^{62a}Nouv. Ann. Math., (4), 11, 1911, 46.

^{62b}Sphinx-Oedipe, 6, 1911, 62.

⁶³Messenger Math., 41, 1911-12, 185-192.

⁶⁴L'intermédiaire des math., 18, 1911, 90-91; 19, 1912, 267-8.

⁶⁵*Ibid.*, 1911, 121, 239.

⁶⁶*Ibid.*, 19, 1912, 26-7, 187.

⁶⁷*Ibid.*, 50-1, 274-9.

⁶⁸*Ibid.*, 77-8, 97.

⁶⁹*Ibid.*, 125, 211.

⁷⁰*Ibid.*, 128.

⁷¹*Ibid.*, 137-9, 202; 20, 1913, 80-81.

⁷²*Ibid.*, 221.

⁷³Il Boll. Matematica Gior. Sc.-Didat., 11, 1912, 233-5.

^{73a}Math. Quest. Educ. Times, (2), 21, 1912, 52-3.

A. Cunningham⁷⁴ listed 63 symmetrical numbers $a_0a_1a_2a_1a_0$ each a product of two symmetrical numbers of 3 digits, and all numbers n^3 , $n < 10000$, and all n^5 , n^7 , n^9 , n^{11} , $n < 1000$, ending with 2, 7, 8, symmetrical with respect to 2 or 3 digits, as $618^3 = 236029032$.

Pairs⁷⁵ of numbers whose l. c. m. equals the product of the digits.

Pairs⁷⁶ of biquadrates, cubes and squares having the same digits.

*P. de Sanctis⁷⁷ noted a property of numbers to the base h^2+1 .

L. von Schrutka⁷⁸ noted that 15, 18, 45 in $7 \cdot 15 = 105$, $6 \cdot 18 = 108$ and $9 \cdot 45 = 405$ are the only numbers of two digits which by the insertion of zero become multiples.

G. Andreoli⁷⁹ considered numbers N of n digits to the base k whose r th powers end with the same n digits as N . Each decomposition of k into two relatively prime factors gives at most two such N 's. If the base is a power of a prime, there is no number >1 whose square ends with the same digits.

Welsch⁸⁰ discussed the final digits of p th powers.

H. Brocard⁸¹ discussed various powers of a number with the same sum of digits.

A. Agronomof⁸² wrote \bar{N} for the number obtained by reversing the digits of N to base 10 and gave several long formulas for $\sum_{j=1}^N \bar{j}$.

The^{82a} only case in which $N^2 - \bar{N}^2$ is a square for two digits is $65^2 - 56^2 = 33^2$. There is no case for three digits.

R. Burg⁸³ found the numbers N to base 10 such that the number obtained by reversing its digits is a multiple kN of N , in particular for $k=9, 4$.

E. Lemoine⁸⁴ asked a question on symmetrical numbers to base b .

H. Sebban⁸⁵ noted that 2025 is the only square of four digits which yields a square 3136 when each digit is increased by unity. Similarly, 25 is the only one of two digits.

R. Goormaghtigh⁸⁶ noted that this property of the squares of 5, 6 and 45, 56 is a special case of $A^2 - B^2 = 1 \dots 1$ (to $2p$ digits), where $A = 5 \dots 56$, $B = 4 \dots 45$ (to p digits). Again, the factorizations $11111 = 41 \cdot 271$, $1111111 = 239 \cdot 4649$ yield the answers 115^2 , 156^2 and 2205^2 , 2444^2 .

⁷⁴L'intermédiaire des math., 20, 1913, 42-44.

⁷⁵Ibid., 80.

⁷⁶Ibid., 124, 262, 283-4.

⁷⁷Atti Accad. Romana Nuovi Lincei, 66, 1912-3, 43-5.

⁷⁸Archiv Math. Phys., (3), 22, 1914, 365-6.

⁷⁹Giornale di Mat., 52, 1914, 53-7.

⁸⁰L'intermédiaire des math., 21, 1914, 23-4, 58.

⁸¹Ibid., 22, 1915, 110-1. Objections by Maillet, 23, 1916, 10-12.

⁸²Suppl. al Periodico di Mat., 19, 1915, 17-23.

^{82a}Sphinx-Oedipe, 9, 1914, 42.

⁸³Sitzungsber. Berlin Math. Gesell., 15, 1915, 8-18.

⁸⁴Nouv. Ann. Math., (4), 17, 1917, 234.

⁸⁵L'intermédiaire des math., 24, 1917, 31-2.

⁸⁶Ibid., 96. Cf. H. Brocard, 25, 1918, 35-8, 112-3.

Several^{86a} gave $9 \cdot n! + n + 1 = 1 \dots 1$ for $n \leq 9$, with generalization to any base.

E. J. Moulton⁸⁷ found the number of positive integers with $r+1$ digits fewer than p of which are unity (or zero). L. O'Shaughnessy⁸⁸ found the number of positive integers $< 10^r$ which contain the digit 9 exactly r times.

Books⁸⁹ on mathematical recreations may be consulted.

F. A. Halliday⁹⁰ considered numbers N formed by annexing the digits of B to the right of A , such that $N = (A+B)^2$, as for $81 = (8+1)^2$. Set $N = A \cdot 10^n + B$. Then $A(10^n - 1) = (A+B)(A+B-1)$, so that it is a question of the factors of $10^n - 1$.

*J. J. Osana⁹¹ discussed numbers of two and three digits.

E. Gelin⁹² listed 450 problems, many being on digits.

^{86a}L'intermédiaire des math., 25, 1918, 44-5.

⁸⁷Amer. Math. Monthly, 24, 1917, 340-1.

⁸⁸Ibid., 25, 1918, 27.

⁸⁹E. Lucas, Arithmétique amusante, 1895. E. Fourrey, Récréations Arithmétiques, 1899.

W. F. White, Scrap-Book of Elem. Math., etc.

⁹⁰Math. Quest. and Solutions, 3, 1917, 70-3.

⁹¹Revista Soc. Mat. Española, 5, 1916, 156-160.

⁹²Mathesis, (2), 6, 1896, Suppl. of 34 pp.

AUTHOR INDEX.

The numbers refer to pages. Those in parenthesis relate to cross-references. Those in brackets refer to editors or translators. The other numbers refer to actual reports.

CH. I. PERFECT, MULTIPLY PERFECT, AND AMICABLE NUMBERS.

- | | | |
|--|---|--|
| <p>Alcafâ, 39
 Alcuin, 4
 Alkalacadi, 40
 Allemanno, 39
 Ankin, 5
 Anonymous, 47
 Aristotle, 38
 Astius, [3]
 Aubry, 31, 33
 Augustinus, 4
 Azulai, 39</p> | <p>De Longchamps, 22
 De Neuveglise, 15
 Desboves, 23, 37 (21, 25)
 Descartes, 12, 33, 34-36, 40-42 (37, 46)
 De Slane, [39]
 De Tovrnes, [8]
 Dickson, 30-32, 49, 50
 Dombart, [4]
 Dupuis, 48</p> | <p>Haas, 48
 Halcke, 41
 Hammond, 30
 Hankel, [4]
 Hansch, 17 (18, 19)
 Harris, 16
 Hebrews, 3
 Heilbronner, 18
 Heinlin, 14
 Henischiib, 10
 Henry, [10, 12, 36, 40]
 Hill, 16 [20]
 Hiller, [3]
 Hoche, [3]
 Hrotsvitha, 5
 Hudelot, 25
 Hultsch, 32
 Hunrath, 43
 Hutton, [16, 18, 19, 36, 47]
 Huygens, [14]</p> |
| <p>Bachet, 10
 Bachmann, 33
 Bæza, 9
 Ball, 12, 32
 Ben Kalonymos, 39
 Ben Korrah, 5, 39
 Bezdiček, 32, 48
 Bickmore, 28
 Boethius, 4 (5-7, 11)
 Bourlet, 28 (29)
 Bovillus, 7 (6, 10, 32)
 Bradwardin, 6
 Brassinne, [12, 36]
 Brocki, 11
 Bronckhorst, 8
 Broscius, 11, 13, 36 (41)
 Bullialdo, [3]
 Bungus, 9, 40 (10-15)</p> | <p>El Madschritt, 39
 El Mağritt, 39
 Eneström, 46
 Ens, 11 (16, 19)
 Escott, 50
 Euclid, 3
 Euler, 17-19, 41-46 (12, 14, 16, 22-28, 31, 47-50)</p> | <p>Iamblichus, 4, 38 (15, 32)
 Ibn Albanna, 40
 Ibn el-Hasan, 39
 Ibn Ezra, 5
 Ibn Khaldoun, 39
 Ibn Motot, 5
 Isidorus, 4</p> |
| <p>Capella, 11
 Cardan, 8, 40 (11, 14)
 Carmichael, 29, 37, 38 (35)
 Carvallo, 22, 24 (26)
 Catalan, 22, 24, 26, 27, 32, 48 (28, 49)
 Cataldi, 10 (7)
 Cesàro, 26
 Chevrel, 27, 48
 Christie, 27
 Chuquet, 6, 40
 Ciamberlini, 29
 Cipolla, 29, 33
 Cole, 29 (13, 22, 25, 27, 32)
 Cunningham, 27, 28, 29, 30, 31, 37, 48 (21, 32)
 Curtze, [6]</p> | <p>Faber Stapulensis, 6 [5]
 Fauquembergue, 27, 30-32 (28, 29)
 Feliciano, 7
 Fermat, 12, 33, 34, 36, 37, 40 (18)
 Ferrari, 33
 Fibonacci (see Leonardo)
 Fitz-Patrick, 27, 33, 48 [28]
 Fontana, 20 (17)
 Fontés, 32 [9]
 Forcadel, 9
 Frenicle, 12, 14, 35 (13, 19, 28, 31)
 Friedlein, [4]
 Frizzo, (4) [8]
 Fuss, 46 [15, 18]</p> | <p>Jacob, 39
 Jordanus, 5 (6, 7)
 Jumeau (see St. Croix)</p> |
| <p>De Backer, [11]
 De la Roche, 8, 40</p> | <p>Genaille, 27
 Gérardin, 29-32, 48-50 (21)
 Gerhardt, [6]
 Ginsburg, [5, 39]
 Giraud, 33
 Goldbach, 15
 Gosselin, [9]
 Gough, 47
 Goulard, 28
 Graevius, [11]
 Grûson, 20, 47 (16)
 Gûdeman, [5]</p> | <p>Kästner, 16
 Kiseljak, 33
 Klügel, 47
 Kraft, 17-19, 41, 50 (8, 9, 20, 46, 47)
 Kraitchik, 22, 25, 47 (32)
 Kummer, [21]</p> |
| | | <p>Landen, 18 (41)
 Landry, 21-23 (25)
 Lantz, 11
 Lax, 7
 Lazzarini, 29
 Lebesgue, 20 (23)
 Lefèvre (see Faber)
 Legendre, 36, 47 (27, 35)
 Lehmer, 37 (36)
 Leibniz, 15</p> |

- Le Lasseur, (21, 23-25, 28, 48)
 Leonardo Pisano, 5
 Leuneschlos, 14
 Leurechon, 11
 Leybourn, 15, 41 [16, 18, 47]
 Libri, [10]
 Liebnecht, 16
 Lionnet, 23 (19)
 Liouville, (19)
 Lucas, 14, 15, 22-25, 27, 28, 37, 40 (12, 17, 19, 21, 29-32, 35, 36, 48)
 Magnin, [5]
 Mahnke, [15]
 Maier, 17 (20)
 Malcolm, 16
 Mandey, [14]
 Mansion, 24, 26
 Manuscript, 6
 Marre, [6]
 Martinus, 7
 Maser, [36, 47]
 Mason, 32, 38
 Maupin, [7]
 Maurolycus, 9 (20)
 McDonnell, 32
 Meissner, 49
 Mersenne, 12, 13, 33, 35, 36, 40, 41 (14, 15, 18, 20, 22, 25, 27, 28, 31, 32)
 Migne, [4]
 Montucla, 19 (16, 36)
 Moret-Blanc, 23
 Munyos, 4
 Nachshon, 39
 Nassò, 32
 Neomagus, 8
 Nicomachus, 3 (4)
 Niewiadomski, 32
 Nocco, 21 (26)
 Novarese, 25 (26)
 Noviomagus, 8
 Oughtred [11]
 Ozanam, 15-17, 36, 41 (19, 20)
 Paciolo, 6, (10, 19)
 Paganini, 47 (49)
 Pauli, 15
 Peacock, 50
 Peletier, 8
 Pellet, 25
 Pepin, 23, 28, 47
 Perrott, 48
 Pervušin, 25
 Philatruss, 15
 Philo, 3
 Pistelli, [4]
 Plana, 21 (17, 22, 24, 29)
 Poggendorff, [11]
 Postello, 9
 Poulet, 50
 Powers, 30, 32 (22)
 Prestet, 15
 Pudlowski, 12
 Puteanus, 11 (14)
 Putnam, 30
 Pythagoreans, 4, 5, 38
 Ramesam, 31
 Ramus, 9
 Recorde, 9, 33
 Regius, 7
 Reuschle, 21 (24, 31)
 Ricalde, 32
 Rubin, [3]
 Rudio, 45
 Ruffus, 7
 Saverien, 19
 Schonero, [9]
 Schooten (see Van)
 Schubert, 32
 Schwenter, 11, 40, 50
 Seelhoff, 25, 48 (29)
 Sempilius, 11
 Semple, 11
 Servais, 26 (25)
 Spoletanus, 7
 St. Croix, 34
 Steinschneider, [5, 39]
 Stern, 25 (19)
 Stifel, 8, 40 (11, 17, 41)
 Stone, 41
 Struve, 20, 47
 Studnička, 28
 Stuyvaert, 28
 Suter, [39]
 Sylvester, 26, 27 (19, 31)
 Tacquet, 14
 Tannery, 28
 Tarry, 30
 Tartaglia, 9, 40 (11, 17)
 Tassius, 15
 Taylor, 20, 50
 Tchebychef, 47
 Tennulius, 15 [4]
 Terquem, 20
 Thâbit (see Ben Korrah)
 Theon of Smyrna, 3
 Turčaninov, 29
 Turschaninov, 29
 Unicornus, 10
 Vaës, 33
 Valentin, 25
 Valla, 6
 Van Etten, 11
 Van Schooten, 14, 41 (42, 47)
 Von Graffenried, 10
 Wantzel, 20 (17)
 Waring, 46
 Wertheim, 33 [10]
 Westerberg, 20
 Westlund, 37, 38
 Willibaldus, 11
 Willichius, 8
 Winsheim, 18 (17)
 Woepeke, [5, 39]
 Wolf, 16 (17)
 Woodall, 30 (28, 32)
 Young, [3]

CH. II. FORMULAS FOR THE NUMBER AND SUM OF DIVISORS, PROBLEMS OF FERMAT AND WALLIS.

- Bang, 56
 Bernoulli, 55
 Blaikie, 58
 Brocard, 57
 Brouncker, 54
 Cantor, 53
 Cardan, 51
 Castillionei, 51
 Chalde, 52
 Cunningham, 58
 Deidier, 52
 De Montmort, 52
 Descartes, 52, 53
 Escott, 54
 Euler, 54
 Fauquembergue, 57
 Fermat, 53, 54, 56 (57)
 Fontené, 52
 Frenicle, 53, 55 (56)
 Genocchi, 57
 Gérardin, 57, 58
 Gerono, 56

Hain, 52
Halcke, 58
Henry, [53, 54, 56]
Hévélius, 54
Hoppe, 51

Kersey, 51
Kraft, 53
Kronecker, 54

Landau, 57
Lionnet, 52, 58
Lucas, 55-58

Mersenne, 51, 53
Minin, 52
Moreau, 57
Moret-Blanc, 57

Newton, 51 (53)

Ozanam, 56

Peano, 53
Plato, 51
Prestet, 52
Pujo, 52

Rudio, 54

Stifel, 51

Vacca, 57
Van Schooten, 51, 55

Wallis, 51, 53-56
Waring, 52, 54, 55
Wertheim, 54
Winsheim, 51
Wolff, 54

CH. III. FERMAT'S AND WILSON'S THEOREMS, GENERALIZATIONS AND CONVERSES; SYMMETRIC FUNCTIONS OF 1, 2, ..., $p-1$ MODULO p .

Allardice, 96
Anton, 75
Anonymous, 67, 70, 92
Arévalo, 83
Arndt, 71, 72 (77, 81, 82)
Arnoux, 81, 94
Aubry, 81, 101 (71, 103)
Axer, 86

Bachmann, 72, 81, 82, 95 (78)
Banachiewicz, 94
Bauer, 88, 89
Beaufort, 62
Beaujeux, 75
Binet, 67
Birkenmajer, 96
Blissard, 74
Borel and Drach, 85, 87 (89)
Bossut, [63]
Bottari, 83
Bouniakowsky, 67, 73, 92, 95
(89, 93)
Brennecke, 69, 73 (80)
Bricard, 81 (75, 82)

Cahen, 80, 103
Candido, 80
Cantor, 62
Capelli, 80, 89
Caraffa, 69
Carmichael, 82, 94 (78, 86,
95)
Carré, 60
Catalan, 71, 77, 98
Cauchy, 67, 69, 70, 95 (86)
Cayley, 76 (75, 83)
Cesàro, 98
Chinese, 59, 91
Cipolla, 93, 94
Concina, 101
Cordone, 85
Crelle, 68, 70, 71, (72)

Cunningham, 94
D'Alembert, 63
Daniels, 78
Dedekind, [74]
De la Hire, 60
Del Beccaro, 79
De Paoli, 67 (79, 82)
D'Escamard, 81
Desmarest, 73
Dickson, 80, 85, 89
Dirichlet, 66, 74 (65, 68, 71,
73, 77, 80, 81, 84)
D'Ocagne, 79, 98
Donaldson, 82
Durege, 73

Earnshaw, 70
Eisenstein, 95
Epstein, (86)
Escott, 93, 94, 103
Euler, 60-65, 92 (66, 67, 69,
72-74, 76, 77, 81-83)

Fergola, 96 (97, 98)
Fermat, 59 (60, 94)
Ferrers, 79, 99
Fontebasso, 74
Franel, 93
Frattini, 84
Frost, 96 (100)

Garibaldi, 77
Gauss, 60, 65, 84 (67, 69, 71,
72, 74, 75, 82, 83, 101)
Gegenbauer, 86, 93, 99
Genese, 78
Genty, 64
Gerhardt, [59]
Glaisher, 99, 100 (102, 103)
Goldbach, 92
Gorini, 70
Grandi, 85

Graves, 73
Gruber, 87
Grunert, 66-68, 71, 72 (65,
73, 81)

Harris, 81
Hayashi, 93
Heal, 77
Heather, 72
Hensel, 91, 101
Horner, 66, 69 (68, 71, 73, 74,
82)

Illgner, 83
Irwin, 103
Ivory, 65 (66-69, 71, 74)

Jacobi, 90 (91)
Janssen van Raay, 101
Jeans, 93 (59, 91)
Jolivald, 93
Jorcke, 76

Kantor, 84
Klügel, [67]
Koenigs, 85
Korselt, 93
Kossett, 93
Kraft, 60
Kronecker, 80, 88

Lacroix, 65, [63]
Lagrange, 62 (59, 64, 73, 74,
97, 99)
Laisant, 75 (76, 78)
Lambert, 61, 92
Laplace, 63 (67, 73, 82)
Lebesgue, 74, 96
Legendre, 64 (80)
Leibniz, 59, 60, 91 (65, 70, 94)
Leudesdorf, 96
LeVavas seur, 88

Levi, 79, 93
 Libri, 69 (101)
 Lindsay, 82
 Lionnet, 71, 98
 Lista, 73
 Lottner, 73
 Lucas, 77, 78, 85, 92, 99 (81,
 82, 86, 93, 94)

MacMahon, 78, 85, 86
 Mahnke, 59, 94 (91)
 Maillet, 78, 85
 Malo, 88, 93
 Mansion, 76
 Maser, [65]
 Mason, 102
 Meissner, 102 (101)
 Meyer, 101
 Midy, 69
 Miller, 81
 Minding, 68 (71, 77)
 Minetola, (66)
 Mitchell, 98, (86, 87)
 Monteiro, 100
 Moore, 87 (88, 89)
 Moreau, 80 (67, 81, 86)
 Morehead, 94
 Moret-Blanc, 98

Nicholson, 81, 101
 Nielsen, 62, 89, 96, 99, 102,
 103 (87) ‡
 Niewenglowski, 96

Osborn, 96, 99
 Ottinger, 75

Peano, [59]
 Pellet, 85

Perott, 80, 88, 99 (75)
 Petersen, 75 (76, 80, 81)
 Petr, 81
 Piccioli, 84
 Picquet, 85
 Pincherle, 80
 Plana, 74
 Poeklington, 82
 Poincot, 71, 95 (72, 76, 101)
 Pollock, 73
 Poselger, 66
 Prompt, 81, 83
 Proth, 92
 Prouhet, 72
 Putnam, 102

Rawson, 99
 Ricalde, 93
 Rieke, 96
 Rogel, 87

Sardi, 74, 97
 Sarrus, 92
 Sauer, 89
 Scarpis, 81, 82
 Schaffgotsch, 64 (65)
 Schapira, 93
 Schering, 76 (80, 81)
 Scherk, 90, 91
 Schlömilch, 73
 Schmidt, 79
 Schönemann, 69, 84
 Schubert, 64
 Schuh, 83
 Schumacher, 83
 Serret, 73, 84, 96 (100)
 Sharp, 96
 Sibirani, 100
 Steiner, 90 (91)

Stern, 74
 Sylvester, 69, 73, 96, 98 (79,
 81, 97)

Talbot, 74
 Tarry, 65
 Tchebychef, 73 (77, 100)
 Terquem, 71
 Thaarup, 92
 Thue, 79, 82
 Toeplitz, 74
 Torelli, 97 (98)
 Tschistjakov, 82

Unferdinger, (75)

Vacca, 59
 Valentiner, 96
 Vályi, 86
 Vandiver, 89, 93
 Verhulst, 66
 Von Schaewen, 76
 Von Staudt, 95
 Von Sterneck, 80

Waring, 62, 64, 95 (81)
 Weber, 80
 Welsch, 95
 Wertheim, 77, 101
 Western, 94
 Westlund, 86, 100
 Weyr, 85
 Wildschütz-Jessen, 84
 Wilson, 62 (59)
 Wolstenholme, 96 (99, 103)

Zeller, 76
 Zsigmondy, 93

CH. IV. RESIDUE OF $(u^{p-1}-1)/p$ MODULO p .

Abel, 105
 Aladow, 107

Bachmann, 109, 111
 Baker, 110
 Bastien, 111
 Beeger, 111
 Brocard, 111

Cunningham, 107, 110

De Romilly, 108
 Desmarest, 105 (106)

Eisenstein, 105 (106)
 Euler, 112 (106)

Fauquembergue, 111

Friedmann, 110
 Frobenius, 110 (111)
 Gegenbauer, 106
 Gérardin, 112
 Glaisher, 108, 109
 Grave, 110 (111)

Hertzer, 110

Jacobi, 105 (111)
 Janssen van Raay, 110
 Lerch, 109, 110 (112)
 Lucas, 106

Meissner, 111, 112 (106, 110)
 Meyer, 107
 Mirimanoff, 107, 110 (109,
 111)

Nielsen, 112

Palmström, 108
 Panizza, 106
 Plana, 106 (109, 112)
 Pleskot, 109
 Pollak, 108
 Proth, 106 (111)

Stern, 106 (109)
 Sylvester, 105 (106-110)

Tamarkine, 110
 Tarry, 111
 Thibault, (105)

Vandiver, 112 (111)
 Verkaart, 111
 Wieferich, 110 (111)

CH. V. EULER'S Φ -FUNCTION, GENERALIZATIONS, FAREY SERIES.

- Airy, 157
 Alasia, 119
 Anonymous, 158
 Arndt, 116, 118 (140)
 Arnoux, 151
 Axer, 138 (157)
 Bachmann, 124, 132, 147, 158
 Bauer, 134
 Berger, 131
 Bernoulli, 140
 Betti, 120
 Binet, 141 (142, 146)
 Blind, 142, 148
 Bonse, 137 (132)
 Borel and Drach, 120, 133
 Bougaief, 142 (145)
 Brennecke, 141 (143)
 Brocot, 156
 Busche, 130, 137, 155, 158
 Cahen, 140, 155, 158
 Cantor, 125 (122, 149)
 Carlini, 136, 150, 153
 Carmichael, 137, 155
 Catalan, 116, 124, 130, 143 (117, 118)
 Cauchy, 116, 140, 156
 Cayley, 121
 Cesàro, 127–130, 143–145, 148–150 (126, 138, 140, 153, 157)
 Chrystal, 120
 Cistiakov, 151
 Composto, 138
 Concina, 131
 Cordone, 155
 Crelle, 115, 117, 140 (118, 119, 121, 132, 137, 139, 141, 143)
 Crone, 125
 Cunningham, 140
 Curjel, 126
 Da Silva, 119, 141
 Davis, 132
 Dedekind, 120, 123 (140)
 Del Beccaro, 146
 De Rocquigny, 124, 143
 Desmarest, 116
 De Vries, 134
 Dirichlet, 119, 122 (121, 126, 127, 130, 132–134, 136, 150, 152, 154)
 D'Ocagne, 157
 Druckenmüller, 116
 Eisenstein, 156
 Elliott, 135
 Euler, 113, 114 (115–118, 122, 138, 146)
 Farey, 156
 Fekete, 137
 Fleck, 139
 Flitcon, 155
 Fontebasso, 122 (120)
 Gauss, 114 (116–118, 122, 133, 142, 147)
 Gegenbauer, 122, 129, 145, 146, 149, 151, 152 (142, 150, 155)
 Glaisher, 146, 148, 157 (150, 158)
 Goldschmidt, 132, 147
 Goodwyn, 156
 Goormaghtigh, 140
 Grunert, 117 (134)
 Guilmin, 119 (118)
 Halphen, 126, 156 (132)
 Hammond, 131, 139, 140, 149 (133)
 Hancock, 139
 Haros, 156
 Harris, 143
 Hensel, 135, 139
 Hermes, 158
 Herzer, 156
 Horta, 119
 Hrabak, 156
 Humbert, 158
 Hurwitz, 158
 Jablonski, 131, 151
 Jensen, 130
 Jordan, 147 (123, 132)
 Kaplan, 134
 Klein, 158
 Knopp, (140)
 Kronecker, 135 (155)
 Kuyver, 139
 Laguerre, 122 (129, 133, 152)
 Landau, 134, 136, 138 (132)
 Landry, 119
 Landsberg, 136
 Lebesgue, 118, 121
 Legendre, 114 (116, 118, 121, 132, 143, 145)
 Lehmer, 153 (157)
 Le Paige, 124
 Lerch, 136
 Leudesdorf, 145
 Liouville, 120, 142 (127, 144)
 Lipschitz, (140)
 Lucas, 125, 131, 142, 147, 157, 158 (123, 126, 137)
 MacMahon, 131
 Made, 158
 Maillet, 134 (132, 137, 138)
 Mansion, 123, 124, 128 (127)
 Mathews, 120
 Mennesson, 143
 Merrifield, 156
 Mertens, 122 (126, 127, 132, 154)
 Métrod, 155
 Miller, 137, 138, 155
 Minding, 116 (118)
 Minin, 133, 155 (140)
 Minine, 124, 143, 144, 157 (145)
 Mitchell, 125
 Moreau, 131, 134 (136)
 Moret-Blanc, 122, 144
 Nasimof, 145 (146)
 Nazimov (Nasimof)
 Nielsen, 146
 Nordlund, 137
 Occhipinti, 136
 Oltramare, 142
 Orlandi, 138
 Orlando, 137
 Pepin, 122 (151)
 Perott, 126 (127, 131)
 Pichler, 134 (137)
 Poinot, 117 (114)
 Poretzky, 130
 Postula, 143
 Prouhet, 118, 140 (131, 150)
 Pullich, 157
 Radicke, 125
 Ranum, 137
 Ratat, 140
 Remak, 138 (132)
 Rogel, 126, 133, 134 (140)
 Sanderson, 155
 Sang, 157
 Scarpis, 139
 Schatunowsky, 132 (134)
 Schemmel, 147
 Sierpinski, 158

- Smith, 122 (123, 124, 127, 128, 130, 136)
 Sommer, 137
 Steggall, 132 (118)
 Stern, 156 (157)
 Story, 148
 Stouvenel, 156
 Sturm, 120
 Suzuki, 137
 Sylvester, 121, 124, 126, 133, 157 (115, 129, 132, 154, 155)
 Tanner, 131
 Tchebychef, 119 (132)
 Thacker, 140 (123, 142, 144-147)
 Tschistiakow, 151
 Vahlen, 133, 158 (157)
 Vályi, 150
 Van der Corput, 139
 Von Ettingshausen, 115 (121)
 Von Schrutka, 158
 Von Sterneek, 151 (153)
 Walla, 126
 Weber, 123, 133, 150
 Weyr, 151
 Wolfskehl, 134 (132, 138)
 Zerr, 140
 Zsigmondy, 132, 152 (145, 146, 155)

CH. VI. PERIODIC DECIMAL FRACTIONS; FACTORS OF $10^n \pm 1$

- Adams, 179
 Akerlund, 176
 Albanna, 159
 Anonymous, 163
 Arndt, 179
 Bachmann, 174, 176
 Barillari, (167)
 Beaujeux, 167 (171)
 Bellavitis, 170
 Bennett, 177
 Bernoulli, 160 (159, 161, 166)
 Bertram, 165 (168)
 Bettini, 175
 Bickmore, 175 (176, 179)
 Biddle, 176
 Bork, 174 (165)
 Bouniakowsky, 171
 Bredow, 163
 Brocard, 165, 172, 174 (159)
 Broda, 169, 172
 Brogtrop, 170
 Burckhardt, 161 (168, 172, 173, 177)
 Carra de Vaux, 159
 Catalan, 164
 Cicioni, 177
 Clarke, 160
 Collins, 166
 Contejean, 173
 Cullen, 176 (179)
 Cunningham, 168, 175-177, 179 (161, 165, 169, 172, 174)
 De Coninck, 168
 Desmarest, 165 (168, 170, 177)
 Dickson, 174
 Dienger, 179
 Druckenmüller, 163
 El-Mâridini, 159
 Escott, 176
 Euler, 160 (165)
 Farey, 162
 Felkel, 161
 Filippov, 177, 179
 Fujimaki, 176
 Gauss, 161 (167, 170)
 Genese, 173
 Genocchi, 165 (160)
 Gérardin, 177 (161, 165)
 Ghezzi, 178
 Glaisher, 162, 166, 168, 170, 171 (173, 175)
 Goodwyn, 161, 162 (170)
 Gosset, 177
 Hartmann, 168
 Hausted, 170
 Heal, 173
 Heime, 166
 Hertzner, 176, 177 (165)
 Hoppe, 179
 Howarth, 179
 Hudson, 166 (167)
 Ibn-el-Banna, 159
 Jackson, 177
 Jenkins, 179
 Johnson, 172
 Kessler, 172, 174 (161, 176)
 Kraitchik, 179
 Kraus, 174
 Kronecker, 176
 Lafitte, 164
 Lagrange, 179
 Laisant, 167, 171, 173
 Lambert, 159 (160, 168) [161]
 Law, 161
 Lawrence, 175
 Lebesgue, 167
 Lehmann, 167
 Leibniz, 159
 LeLasseur, 172
 Leman, 179
 Levänen, 179
 Lichteneker, 178
 Lionnet, 167
 Loof, 165, 171, 172, 175 (168)
 Lucas, 159, 171, 172, 175, 177 (176)
 Lugli, 172
 Mahnke, 159
 Maillet, 178
 Mansion, 169
 Mayer, 173, 174
 Meyer, 167 (176)
 Midy, 163 (164, 166)
 Mignosi, 177
 Miller, 176
 Mörrck, 179
 Morel, 167
 Moret-Blanc, 168
 Muir, 168, 169
 Murer, 175
 Nordlund, 176
 Oberreit, 161
 Oliver, 166
 Pasternak, 178
 Pellet, 167
 Perkins, 163 (176)
 Pokorny, 166
 Poselger, 162
 Prouhet, 164
 Reuschle, 165, 169 (172, 174, 176)
 Reyer, 165
 Reynolds, 175
 Rieke, 173
 Robertson, 159 (160)
 Sachs, 175
 Salmon, 168
 Sanio, 167
 Sardi, 167 (175)
 Schlömilch, 171 (172)
 Schröder, 168
 Schröter, 161
 Schuh, 177
 Seelhoff, 160
 Sensenig, 169
 Shanks, 168, 170 (161, 165, 169, 176)

Sornin, 164
 Stammer, 166
 Stasi, 178
 Sturm, 166
 Suffield, 166

Tagiuri, 176

Telosius, 179
 Thibault, 164 (168)
 Van den Broeck, 172
 Van Henekeler, 165

Wallis, 159 (160)
 Weixer, 179

Welsch, 179
 Wertheim, 161
 Westerberg, 163
 Wiley, 179
 Workman, 176 (168)
 Wucherer, 161
 Young, 165

CH. VII. PRIMITIVE ROOTS, BINOMIAL CONGRUENCES.

Alagna, 217 (218)
 Alasia, 190 (210)
 Allegret, 190
 Amici, 197, 216, 217
 Anonymous, 204
 Arndt, 187, 188, 208, 209
 (193)
 Arnoux, 199, 218

Bachmann, 194, 199, 218
 Barillari, 192 (193)
 Barinaga, 203
 Bellavitis, 193
 Bennett, 195
 Berger, 214 (215)
 Besant, 217
 Bhāscara, 204
 Bindoni, 199
 Bougaief, 213
 Bouniakowsky, 191, 192, 212
 (204)
 Brennecke, (208)
 Bukaty, 212 (210)
 Burekhardt, (185, 201)
 Buttel, 190

Cahen, 198
 Calvitti, (204)
 Carmichael, 200, 202
 Cauchy, 184, 186, 187, 209
 (188, 190, 194, 195, 198,
 200, 212, 213)

Cayley, 191
 Chabanel, 202
 Christie, 199
 Cipolla, 200, 218–221
 Colebrooke, [204]
 Concina, 222
 Contejean, 194
 Creak, 222
 Crelle, 185, 209 (186, 188,
 190, 208)
 Cunningham, 198–204, 217–
 222 (185, 189, 190, 213)

Daniëls, 194
 Da Silva, 190, 210
 De Jonquières, 197
 Demeczky, 201

Desmarest, 188, 189, 210
 (214)
 Dickstein, 210, 215
 Dirichlet, 185, 191, 211 (198,
 214)
 Dittmar, 212
 Dupain, 192

Epstein, 200
 Erlerus, 186, 208 (196)
 Euler, 181, 204, 205 (222)

Foglini, 199
 Fontené, 201
 Forsyth, 193
 Frattini, 193
 Frégier, 183
 Friedmann, 219
 Frolov, 196

Gauss, 182, 194, 195, 207
 (183–185, 187, 188, 193,
 194, 197, 198, 209, 210, 213,
 214)

Gazzaniga, 213
 Gegenbauer, 194, 196, 215
 Gérardin, 222
 Goldberg, 192
 Gorgas, 211
 Grave, 201
 Grigoriev, 199
 Grosschmid, 221

Hacken, 194
 Hanegraeff, 210
 Heime, 191
 Hill, 192
 Hofmann, 193
 Hoüel, 191
 Hurwitz, (203)

Ivory, 184 (190)

Jacobi, 185 (188, 190–192,
 198, 201, 203, 211)
 Japanese, 204

Kefenstein, 194
 Korkine, 201 (203, 221)

Kraitchik, 202
 Krediet, 203
 Kronecker, 192, 198
 Kulik, 189
 Kunerth, 213

Lacroix, 183 [208]
 Ladrasch, 212
 Lagrange, 181, 205 (182, 206,
 207, 214, 216)
 Laisant, 193
 Lambert, 181
 Landau, 201
 Landry, 190
 Laplace, 208
 Lazzarini, (222)
 Lebesgue, 184, 188–192, 208,
 211 (196, 204)
 Legendre, 182, 205–207 (185,
 187, 188, 194, 208, 213–
 215, 219, 222)
 Leibniz, 215
 Libri, 208
 Lucas, 194, 213 (198, 200,
 202, 203, 218)

Maillet, 202
 Mann, 215
 Marcolongo, 214
 Maser, [182, 206, 207]
 Massarini, 188
 Mathews, 195, 215
 Matsunaga, 204
 Maximoff, 222
 Mayer, 216
 Meissner, 219
 Mertens, 198 (192)
 Meyer, 211
 Miller, 198, 201, 203
 Minding, 185
 Moreau, 198
 Murphy, 186

Nordlund, 200

Oltramare, 189, 190 (191)
 Ostrogradsky, 185 (186, 188)

Pepin, 197, 213

Perott, 194, 196, 197
 Picou, 218
 Pocklington, 222
 Poinset, 183, 184, 187, 208,
 209 (190, 194, 199, 207,
 208)
 Posse, 201, 202, 203, 221
 Prouhet, 188 (194, 208)

 Rados, 222
 Reuschle, 190, 213 (200, 204)
 Richelot, 185 (194)
 Rochette, 188

 Sancery, 193, 213 (194, 195)
 Schapira, 188

Scheffler, 190, 194
 Schering, (208)
 Schuh, 202 (221)
 Schumacher, 202
 Schwartz, 194
 Seelhoff, 214
 Serret, 194, 214
 Smith, 191, 210 (184, 190,
 207)
 Speckmann, 216, 217
 Stankewitsch, 213
 Stasi, 221
 Stern, 184, 208 (187, 194, 199,
 203)
 Studnička, 215
 Szily, 194

Tamarkine, 219
 Tchebychef, 188 (185, 191,
 195, 196, 198, 207)
 Thiele, 212
 Tonelli, 215, 216 (217, 218)
 Traub, 192

 Valroff, 222
 Von Schrutka, 202, 221

 Wertheim, 194, 196, 197, 199,
 214 (201, 202)
 Woodall, 203 (202)
 Wronski, 210 (211, 212, 215,
 218)
 Zsigmondy, 195, 197, 216

CH. VIII. HIGHER CONGRUENCES.

Abel, 259
 Alasia, 224
 Arnoux, 250, 251, 254 (255)

 Bachmann, 250, 251
 Bauer, 249, 251
 Bellavitis, 244
 Biase, 260
 Borel and Drach, 247
 Bunickij, 260
 Bunitzky, 260
 Bussey, 251

 Cailler, 255, 256
 Carey, 249
 Cauchy, 223, 225, 238, 252,
 258 (243)
 Châtelet, 262
 Christie, 262
 Cipolla, 232
 Cordone, 247, 254, 259
 Creak, 262
 Crelle, 223 (224)
 Cunningham, 262

 Damm, 247, 254
 Da Silva, 224
 Dedekind, 240, 245 (242)
 Demeczky, 228
 Dickson, 232, 248-250, 252,
 254, 256 (244, 249)
 Dina, 246

 Earnshaw, 223
 Eisenstein, 239
 Epstein, 250 (249)
 Escott, 256
 Euler, 223 (259)

 Fermat, 257 (260)
 Frattini, 259, 261

 Galois, 235 (232, 239, 242,
 243, 247, 252)

Gauss, 223, 233 (235, 238,
 240, 256)
 Gegenbauer, 226-229, 231
 Genocchi, 258
 Giudice, (259)
 Gröttsch, 261
 Grunert, 224
 Guldberg, 248, 250

 Hathaway, 259
 Hayashi, 256
 Hensel, 226, 249
 Hermite, 225
 Hurwitz, 231, 259 (232, 233)

 Iwanow, 254

 Jacobi, 235
 Jenkins, 259
 Jordan, 243, 244, 261 (252)

 Kantor, 255, 262
 König, 225 (226, 229)
 Krediet, 261
 Kronecker, 226, 249, 260
 (228, 229, 251)
 Kühne, 232

 Lagrange, 223
 Landau, 261
 Lebesgue, 224, 235, 258 (245)
 Legendre, 223, 257
 Lerch, (227, 228)
 Le Vavasseur, 248
 Libri, 224 (225, 258)
 Lipschitz, 260 (257)

 Maser, [223, 233, 235]
 Mathieu, 241 (248)
 Miller, 251
 Mirimanoff, 255
 Mitchell, 246
 Moore, 247

Neikirk, 251

 Oltramare, 253 (254)

 Pellet, 243, 245, 246
 Pepin, 244
 Piccioli, 261
 Pierce, 262
 Poinset, 224 (259)

 Rados, 226, 233, 261, 262
 (225)
 Raussnitz, 226

 Sanderson, 252
 Satunovskij, 231
 Scarpis, 252
 Schönemann, 225, 236, 238,
 239 (251)
 Schütz, 243
 Schwacha, 233
 Serret, 239, 241, 244, 258
 (233, 245, 246, 248, 256)
 Smith, 241, 259
 Snopek, 229
 Stephan, 232
 Stickelberger, 249 (251)
 Sylvester, 259 (245)

 Tarry, 252
 Tchebychef, 225
 Tihanyi, 262

 Von Sterneck, 255, 260, 261
 (262)
 Voronoï, 251, 253 (255)

 Weber, 247
 Wertheim, 260
 Woodall, 262
 Woronoj, 253, 254
 Wronski, 257

 Zsigmondy, 230, 247

CH. IX. DIVISIBILITY OF FACTORIALS, MULTINOMIAL COEFFICIENTS.

- Adams, 278
 André, 263, 265-6
 Anonymous, 275
 Anton, 263, 271
 Arévalo, 278
 Arndt, 276 (277)

 Babbage, 270
 Bachmann, 266, 274
 Bauer, 268
 Beaujeux, 277
 Beeger, 278
 Bernoulli (268)
 Bertram, 263
 Birkeland, 269
 Bouniakowsky, 276-7
 Bourguet, 266

 Carmichael, 264, 276, 278
 Catalan, 265-7, 271-2
 Cauchy, 265
 Cayley, 269, 270
 Cesàro, 266, 272
 Child, 278
 Cunningham, 265, 274

 De Brun, 263
 De Jonquières, 270
 De Polignac, 266, 269
 De Presle, 267
 Dickson, 273 (272)
 Dirichlet, 275 (276)

 Elliott, 270

 Fleck, 274-5
 Fontené, 274
 Franel, 276

 Gauss, 269
 Gegenbauer, 267, 272
 Genocchi, 271
 Genty, 263

 Gerhardt, [269]
 Glaisher, 268, 273-4
 Gmeiner, 267
 Greatheed, 269
 Grosschmid, 274
 Guérin, 275

 Hayashi, 274
 Heine, 267
 Hensel, 263
 Hermite, 266, 271-2 (267, 269, 274)
 Jacobi, 275 (276)
 Jänichen, 265
 Jenkins, 269, 271

 Kapferer, 274
 Kempner, 263
 Korkine, 276
 Kronecker, 276
 Kummer, 270 (272-3)

 Lagrange, 275
 Laisant, 277
 Landau, 267-9
 Lebesgue, 269
 Legendre, 263 (264)
 Leibniz, 269 (270)
 Lerch, 276
 Libri, 270
 Liénard, 266
 Lionnet, 269
 Liouville, 276
 Lucas, 266, 271-2, 275 (274, 278)

 MacMahon, 268
 Maillet, 265, 268
 Maitra, 269
 Malo, 276
 Marks, 278
 Mason, 278

 Mathews, 272-3
 Mertens, 273
 Miller, 269
 Morley, 273

 Neuberg, 263, 266
 Nielsen, 274, 278

 Oltramare, 277
 Ouspensky, 276

 Pascal, 269
 Pessuti, 269
 Petersen, 272
 Pincherle, 267

 Ram, 274
 Rogel, 267, 272

 Schlömilch, 272
 Schönbaum, 269
 Schönmann, 265
 Segar, 269 (270)
 Sharp, 272
 Stern, 270
 Stickelberger, 263
 Stridsberg, 264, 269
 Studnička, 270
 Szegő, 265
 Szily, 273

 Tanner, 267
 Teixeira, 267, 277
 Thue, 267

 Van den Broeck, 272
 Vandiver, 276
 Vecchi, 277

 Waring, 275
 Weill, 266 (267-8)
 Wolstenholme, 271-2 (275)
 Woodall, 272

CH. X. SUM AND NUMBER OF DIVISORS.

- Ahlborn, 291
 Andreievsky, 288

 Bachmann, 279, 315, 321, 323 (281, 291, 319)
 Bell, 323, 325
 Berger, 291, 312, 317 (292, 295, 299)
 Bougaief, 303, 315 (301, 312, 316, 325)
 Bouniakowsky, 283, 284, 287 (281, 286, 302)

 Burhenne, 283
 Busche, 306, 308, 314, 319 (315, 323)
 Cantor, 291
 Catalan, 289-291, 302, 306 (292, 295)
 Cesàro, 290-4, 302, 306, 308 (295, 298-9, 312, 315, 320)
 Cunningham, 325
 De Vries, 317

 Dirichlet, 281-2, 301 (284-5, 289, 291, 298-9, 305, 307, 314-5, 318, 322, 325)

 Egorov, 312
 Elliott, (318)
 Euler, 279 (284, 290, 303, 312, 317-8, 321, 323)

 Fekete, 321
 Fergola, (302)
 Franel, 317-8

- Gauss, 308
 Gegenbauer, 298-9, 301-5, 307-8, 316 (288, 315, 318, 325)
 Giuliani, 319
 Glaisher, 289-292, 294-6, 300, 303-4, 308-310, 312, 318, 320, 322 (280, 302, 321)
 Gram, 295, 308 (291)
 Gronwall, 322

 Hacks, 306-7 (303, 322)
 Halphen, 289, 290 (294-5, 309, 312)
 Hammond, 311 (325)
 Hansen, 319
 Hardy, 325 (319)
 Hemming, 284
 Hermite, 292, 295, 297, 306 (304-5, 315)

 Jacobi, 281-2 (283, 288, 290, 295, 300-1, 313, 317-8)

 Knopp, 321, 323
 Kronecker, 297, 318

 Laisant, 308

 Lambert, 280 (306, 323)
 Landau, 294, 305, 317-8, 321-4
 Lebesgue, 284
 Legendre, 281
 Lerch, 307, 313, 316 (314-5, 317)
 Lionnet, 288
 Liouville, 284-8 (291-4, 298-9, 312-3, 321, 323)
 Lipschitz, 291-2, 298, 302 (299, 307, 313, 315)
 Lucas, 291, 312

 Meissel, 284 (299, 314, 317-8, 322)
 Meissner, 320
 Mellin, 319
 Mertens, 289 (294, 315)
 Minetola, 322
 Minin, 313
 Möbius, 296

 Nachtikal, 316

 Pexider, 320
 Pfeiffer, 305 (322)
 Piltz, 291 (317, 322, 325)
 Plana, (281)

 Radicke, 291
 Ramanujan, 323-5
 Roberts, 303
 Rogel, 316, 325
 Runge, 302

 Sardi, 288
 Schröder, 314, 319, 321 (315)
 Sierpinski, 320
 Smith, 289 (296)
 Sokolov, 312
 Steffensen, 323
 Stern, 281, 303 (321)
 Stieltjes, 292
 Strnad, 307

 Traub, 287

 Vahlen, 313
 Van der Corput, 323-4
 Von Mangoldt, 294
 Von Sterneek, 317
 Voronoï, 318-9 (322, 325)

 Waring, 280 (303)
 Wigert, 320, 323, 325

 Zeller, 291, 295, 313 (299, 303, 312, 321)

CH. XI. MISCELLANEOUS THEOREMS ON DIVISIBILITY, GREATEST COMMON DIVISOR, LEAST COMMON MULTIPLE.

- Anonymous, 327
 Avery, 332
 Axer, 331

 Bachmann, 335
 Barinaga, 336
 Berger, 328
 Binet, (332)
 Birkeland, 331
 Borel, 334 (333)
 Bougaief, 327 (328, 330)
 Bouniakowsky, 332
 Brown, 336

 Cesàro, 328, 333 (336)

 Darbi, 335
 Dedekind, 334
 De Jough, 335
 De la Vallée Poussin, 330 (331)
 De Polignac, 336
 Dickson, 331
 Dienger, 327
 Dintzl, 335
 Dirichlet, 327, 335 (328-331)
 Dupré, (332)

 Gegenbauer, 328-330, 333, 336
 Gelin, 335
 Grolous, 328
 Guzel, 331

 Hacks, 330, 333
 Hammond, 333
 Hensel, 334 (333)

 Klein, 334
 Kluyver, 335
 Kronecker, 334 (336)

 Lamé, (332)
 Landau, 328, 331
 Lebesgue, 332 (335)
 Lecat, 336
 Lucas, 333

 Mertens, 334-5
 Mitchell, 336
 Moschietti, 332

 Neuberg, 333

 Pichler, 335

 Rogel, 331
 Ross, 336
 Rothe, 332

 Saint-Loup, 330
 Sierpinski, 335
 Stern, 335
 Stieltjes, 333
 Stifel, 327
 Sylvester, 327, 333, 336

 Terquem, [327]

 Van der Corput, 332
 Vandiver, 331
 Verhagen, 336
 Verson, 332

 Weitbrecht, 332
 Wijthoff, 336
 Willaert, 336

 Yanney, 335

 Zeller, 328

CH. XII. CRITERIA FOR DIVISIBILITY BY A GIVEN NUMBER.

- Adam, 345
 Alkarkhi, 337
 Anonymous, 339, 344
 Anton, 345
 Apianus, 337
 Argardh, 338
 Avicenna, 337
 Ayza, 346

 Badoureau, 345
 Barlow, (346)
 Bělohlávek, 342
 Biase, 343
 Biddle, 345
 Bindoni, 343
 Börgen, 342
 Bougaief, 340 (342)
 Bougon, 341
 Bouniakowsky, 344
 Breton, 341
 Broda, 345
 Brooks, 345
 Bruzzone, 344
 Burgess, 345
 Buttel, 344

 Calvitti, 345
 Cantor, [337]
 Carra de Vaux, 337
 Castelvetro, 338
 Catalan, 340
 Cattaneo, 346
 Cazes, 345
 Cesàro, 345
 Chiari, 344
 Christie, 341, 345
 Chuquet, 337
 Church, 345
 Cicero, 346
 Collins, 345
 Conti, 345
 Crelle, 339
 Csada, 346
 Cunningham, 345

 D'Alembert, 338 (344)
 Da Ponte Horta, 345
 De Fontenelle, 338
 De Lapparent, 344
 Delboeuf, 340
 De Montferrier, 344
 Dickstein, 341, 345
 Dietrichkeit, 341
 Dietz, 344
 Dodgson, 342
 Dörr, 345
 Dorsten, 345

 Dostor, 340
 Drach, 345
 Dupain, 339

 Elefanti, 344
 Elliott, 339
 Evans, 345

 Fazio, 345
 Filippov, 346
 Flohr, 344
 Folie, 339
 Fontebasso, 346
 Fontès, 341-2 (337)
 Forcadel, 337

 Galé, 346
 Gelin, 343, 345
 Gérardin, 345
 Gergonne, 338 (345)
 Ghezzi, 345
 Gorini, 344
 Greenfield, 345
 Greenstreet, 345
 Grunert, 344

 Haas, 345
 Harmuth, (346)
 Heal, 342
 Heilmann, 341
 Herter, 338 (344)
 Hill, 338
 Hippolytos, 337
 Hočevár, 340
 Holten, 340
 Hommel, 340

 Ibn Albannâ, 337
 Ibn Mûsâ Alchwarizmî, 337
 Ibn Sînâ, 337
 Ingleby, 345
 Iodi, 346

 Jenkins, 345
 Jorcke, 345
 Joubin, 346

 Karwowski, 344
 Kraft, 338
 Krahl, 346
 Kroupa, 346
 Kylla, 346

 Lagrange, 338
 Lalbaletrier, 345
 La Marca, 346
 Lange, 345

 La Paglia, 346
 Lebesgue, 344
 Lebon, (346)
 Lenthéric, 346
 Lenzi, 345
 Leonardo Pisano, 337
 Levänen, 341
 Lichtenecker, 346
 Liljevalch, 338 (340)
 Lindman, 344
 Loir, 341-2, 345
 Loria, 343
 Lubin, 345

 Malengreau, 343
 Mantel, 340
 Marianтони, 345
 Marre, [337]
 Mason, 344
 Meissner, 343
 Mennesson, 345
 Miceli, 346
 Möller, 340
 Morale, 345-6

 Nannei, 344
 Nassò, 345
 Niegemann, 339, 344
 Niewenglowski, 345
 Noël, 341

 Oskamp, 340
 Otto, 340

 Paciulo, 337
 Paoletti, 346
 Pascal, 337 (338, 342, 344-5)
 Perisco, 346
 Perrin, 341
 Pick, 345
 Pietzker, 345
 Pinaud, 344
 Plakhowo, 342
 Polpi, 346

 Recorde, 337
 Reyer, 344
 Riess, 342
 Ripert, 343
 Romm, [337]

 Sanvitali, 338
 Schlegel, 340 (345)
 Schobbens, 341
 Schröder, 346
 Schuh, 344
 Sibt el-Mâridini, 337
 Speckmann, 345

Stouff, 345
 Stuyvaert, 344
 Sylvester, 342
 Szenic, 345

Tagiuri, 343
 Tarry, (346)
 Terquem, 344
 Tiberi, 346
 Tirelli, 346

Transon, 339
 Tucker, 341

Unferdinger, 345

Valerio, 342
 Van Langeraad, 344
 Vincenot, 344
 Volterrani, 346

Walenn, 345
 Wertheim, 345
 Widmann, 337
 Wilbraham, 339
 Wronski, 344

Young, 344

Zbikowski, 339
 Zeipel, 339
 Zuccagni, 345

CH. XIII. FACTOR TABLES, LISTS OF PRIMES.

Akerlund, 355
 Alliston, 356
 Anjema, 348
 Aratus, 347
 Aubry, 355

Barlow, 351 (355)
 Beguelin, 349
 Bernhardt, 347
 Bernoulli, 349 [350]
 Bertelsen, 354
 Bertrand, 349
 Boethius, 347
 Boulogne, 356
 Bouniakowsky, 353
 Bourgerel, 354
 Brancker, 347 (348, 350)
 Burckhardt, 350 (352-5)

Camerarius, 347
 Cataldi, 347
 Cayley, 353
 Chernac, 350 (351)
 Colombier, 351
 Crelle, 351-2
 Cunningham, 354-5 (350-2, 356)

D'Alembert, 349
 Dase, 352 (353-5)
 Davis, 352
 De Polignac, (356)
 Deschamps, 355
 Desfaviaae, 350
 De Traytorens, 348 (350)
 Di Girio, 354
 Dines, 355
 Dodson, 348
 Du Tour, 348

Eratosthenes, 347 (348, 353-6)
 Escott, 355 (356)
 Euler, 349 (356)
 Felkel, 349, 350

Gauss, 350, 352 (356)
 Gérardin, 356
 Gill, 353
 Glaisher, 350, 353 (355)
 Goldberg, 352
 Gram, 354
 Groscurth, 353
 Grison, 350
 Gudila-Godlewski, 353
 Guyot, 351

Hansen, 356
 Hantschl, 351
 Harris, 348
 Hindenburg, 349
 Hinkley, 351 (347)
 Horsley, 347
 Houël, 351-2
 Hülse, [350]
 Hutton, 351

Ibn Albannâ, 347

Jäger, 348
 Johnson, 353
 Jolivald, 354

Kästner, 350
 Kempner, (356)
 Klügel, 348
 Köhler, 351
 Krause, 350
 Kronecker, (354)
 Krüger, 348
 Kulik, 351 (355-6)

Laisant, 354-5
 Lambert, 348, 350 (349)
 Landry, 351
 Lebesgue, 352
 Lebon, 355-6
 Lehmer, 352-3, 355-6
 Leonardo Pisano, 347
 Libri, 347
 Lidonne, 350

Lionnet, 355
 Lucas, 353

Marci, 349
 Marre, [347]
 Maseres, 350
 Meissel, 352 (350)
 Merlin, (356)
 Möbius, 351
 Morehead, 355

Neumann, 350
 Nicomachus, 347
 Noviomagus, (356)

Oakes, 352
 Oberreit, 349
 Ozanam, 349

Pell, [347]
 Perott, 352
 Petzval, 352
 Pigri, 348
 Poetius, 348
 Poretzky, (356)

Rahn (Rhonius), 347
 Rallier des Ourmes, 348
 Rees, 351
 Reymond, (356)
 Rosenberg, 352 (355)
 Rosenthal, 349

Saint-Loup, 353 (356)
 Salomon, 351
 Schaffgotsch, 349
 Schallen, 351
 Schapira, 354
 Schenmarck, 350
 Schwenter, 348
 Seelhoff, 353
 Simony, 353 (354)
 Snell, 350
 Speckmann, 354
 Stager, 356
 Struve, 350
 Suchanek, 354

Tarry, 355
 Tennant, 354
 Tessanek, 349
 Tuxen, 353
 Valerio, 354

Van Schooten, 347
 Vega, 350
 Vollprecht, 353-4
 Von Stamford, 349
 Von Sterneek, 354

Wallis, 348 (347)
 Wertheim, [347]
 Willigs (Willich), 348
 Wolf, 348
 Woodall, 354 (356)

CH. XIV. METHODS OF FACTORING.

Aubry, 373 (369)
 Ball, 368
 Barbette, 367, 373
 Bartl, 370
 Beguelin, 361, 366
 Bernoulli, 371
 Bickmore, 369
 Biddle, 359, 367, 369-374
 Birch, 368
 Bisman, 374
 Bouniakowsky, 369 (370)
 Burgwedel, 365
 Busk, 358 (359)
 Cahen, 364
 Canterzani, 366
 Cantor, [366]
 Christie, 361, 367, 372
 Cole, 365
 Collins, 357
 Cullen, 365, 369
 Cunningham, 358-9, 361,
 365, 368-9, 373-4 (362)
 De Bessy (see Frenicle)
 De Montferrier, 358
 Deschamps, 367
 Dickson, 370 (360)
 Euler, 360-2 (363-5)
 Fermat, 357 (358, 367)
 Frenicle, 360
 Fuss, 362
 Gauss, 363, 369 (364-5, 370)
 Gérardin, 365-7, 370, 374

Gmeiner, 374
 Gough, 371
 Grube, 363
 Hansen, (371)
 Harmuth, 361
 Henry, 358
 Hudson, 358
 Johnsen, 369
 Joubin, 372
 Kausler, 357, 362
 Kempner, 374
 Kielsen, 372
 Klügel, 366
 Kraft, 370
 Kraitchik, 359, 360
 Kulik, 361, 372
 Lagrange, 369
 Lambert, 371
 Landry, 358, 369, 371
 Laparewicz, 365
 Lawrence, 358-360
 Lebon, 359, 373
 Legendre, 361-2 (363)
 Lehmer, 368
 Levänen, 364
 Lucas, 363-4 (372)
 Märcker, 368
 Mathews, 364
 Matsunaga, 371
 Meissner, 372 (358, 364, 367)
 Mersenne, 357, 360 (367-8)
 Meyer, 365
 Minding, 363

Möbius, (374)
 Neumann, 359
 Niegemann, 366
 Nordlund, 370-1 (369)
 Pepin, 364
 Petersen, 360
 Pocklington, 370
 Rawson, 367
 Reymond, 374
 Schaffgotsch, 367
 Schatunovsky, 370
 Seelhoff, 363 (365)
 Seliwanoff, 364
 Speckmann, 367
 Studnička, 366
 Tchebychef, 363
 Teilhet, 359
 Tessanek, 366
 Thaarup, 358
 Thielmann, 368
 Vaes, 359, 360
 Valroff, 365
 Von Segner, 366
 Vuibert, 361
 Waring, 362
 Warner, 358
 Weber, 364
 Wertheim, 358, 361
 Winter, 372
 Woodall, 369

CH. XV. FERMAT NUMBERS $F_n = 2^{2^n} + 1$.

Anonymous, 376
 Archibald, 380
 Bachmann, 379
 Ball, 378
 Baltzer, 375
 Beguelin, 375 (377)
 Bisman, 379
 Broda, 377
 Canterzani, 375

Carmichael, 377, 380
 Catalan, 377
 Cipolla, 378
 Cullen, 378
 Cunningham, 378-380
 Eisentein, 376
 Euler, 375
 Fermat, 375 (376)
 Frenicle, 375

Gauss, 375
 Gelin, 377
 Genocchi, 375
 Gérardin, 377, 380
 Goldbach, 375
 Gosset, 379
 Hadamard, 378
 Henry, 375, 380
 Hermes, 378
 Hurwitz, 378 (380)

- | | | |
|--------------------|----------------------|------------------|
| Joubin, 376 | Malvy, 378 (376) | Proth, 377 (378) |
| Klein, 378 (379) | Mansion, 375 | Scheffler, 378 |
| Klügel, 375 | Mersenne, 375 | Seelhoff, 377 |
| Landry, 376-7 | Morehead, 376, 379 | Simerka, 377 |
| Legendre, (378) | Nazarevsky, 378 | Studnička, 377 |
| Le Lasseur, 377 | Pepin, 376 (377-380) | Western, 378-9 |
| Lipschitz, 378 | Pervouchine, 376-8 | Woodall, 379 |
| Lucas, 376-8 (379) | Pervusfn, 376 | |

CH. XVI. FACTORS OF $A^n \pm B^n$.

- | | | |
|--------------------------------|------------------------------|------------------------|
| Aurifeuille, 383 (386) | Gauss, 382 | Pepin, 384-6 |
| Bang, 385 (386) | Genese, 385 | Plana, 383 |
| Bauer, 385 | Gérardin, 390 | Pocklington, 390 |
| Beguelin, 381 (385) | Germain, 382 (383) | Réalis, 384 |
| Bickmore, 386 (385) | Gianni, 385 | Reuschle, 382-3 |
| Biddle, 387 (391) | Glaisher, 386, 388 | Sanjana, 389 |
| Birkhoff, 388 (386) | Henry, 382 | Scheffler, 385 |
| Carmichael, 389, 390 (388) | Kannan, 389 | Schering, 382 |
| Catalan, 383-4 (386) | Kraitchik, (391) | Seelhoff, (391) |
| Cunningham, 386-391 (384) | Kronecker, 385, 387 | Soons, 383 |
| Dedekind, 384 | Kummer, 383 | Sylvester, 384-5 |
| Dickson, 388-9 | Lawrence, (391) | Tchebychef, 382 |
| Dines, (391) | Lebesgue, 382-3 | Teilhet, 388 |
| Dirichlet, (391) | Lefébure, 384 | Valroff, 390 |
| Escott, 385, 387-9 | Legendre, 382 | Van der Corput, 390 |
| Euler, 381-2 (383, 388, 390-1) | Le Lasseur, 383 (384-5, 389) | Vandiver, 387-8 |
| Fauquembergue, 390 | Lucas, 383-4, 386 | Welsch, 389 |
| Felkel, 382 | Markoff, 386 | Wertheim, 388 |
| Fermat, 381 | Minding, 382 | Woodall, 386, 388, 391 |
| Fontené, 390 | Miot, 389 | Workman, 386 |
| Foster, 385 | Morehead, (391) | Zsigmondy, 386 (388) |

CH. XVII. RECURRING SERIES; LUCAS' u_n, v_n .

- | | | |
|----------------------|---------------------------------|------------------------------|
| Agronomof, 406 | Braun, 411 | Degen, 407, 411 |
| Amsler, 410 | Brocard, 402 | De Longchamps, 401, 408 |
| André, 408 | Candido, 405 | De Moivre, 407 |
| Archibald, 411 | Cantor, [407] | Dickson, 405, 410 |
| Arista, 405 | Carmichael, 394, 406 (398, 400) | Dienger, 394 |
| Arndt, (397) | Cassini, 407 | Dirichlet, 393 (402) |
| Aubry, 405 | Catalan, 395, 402-3 (404) | D'Ocagne, 402, 409, 410 |
| Bachmann, 394, 405 | Cesàro, 401-2 | Emmerich, 404 |
| Bastien, 406 | Christie, 404 | Escott, 404-5 |
| Bernoulli, 407 (408) | Cipolla, 405 | Euler, 393, 407 (397-8, 400) |
| Betti, 408 | Cunningham, 397 | Fermat, (396) |
| Bickmore, 404 | Damm, 405 | Fibonacci (see Leonardo) |
| Binet, 394 (403) | | Fontès, 403 |
| Boutin, 406 | | |

- Foster, 403
 Fourier, 408
 Fransen, 405
 Frisiani, 408
 Frolov, 403

 Galois, (403)
 Gauss, 393 (397)
 Gegenbauer, 403, 409
 Gelin, 401
 Genocchi, 394, 397, 402 (405)
 Gérardin, 406
 Girard, 393
 Grosschmid, 394

 Hayashi, 410
 Hill, 394

 Kepler, (411)
 Kronecker, 402 (393)

 Lagrange, 393, 407 (396-7, 408)
 Laisant, 408, 410
 Lamé, 394
 Landau, 404-5
 Laparewicz, 405
 Laplace, 407
 Lattès, 410
 Legendre, 393
 Le Lasseur, 400
 Leonardo Pisano, 393 (394-411)

 Liebetruith, 402
 Lionnet, 394
 Lucas, 394-403 (405-6)

 Magnon, 402
 Maillet, 403, 410
 Malfatti, 407
 Malo, 404, 406
 Mantel, 403
 Mathieu, 405
 Mersenne, (397)
 Moret-Blanc, 397
 Murphy, 408

 Netto, 410
 Neuberg, 410
 Nicita, 411
 Niewiadomski, 406

 Paoli, 407
 Pellet, 406
 Pepin, 398, 401
 Perrin, 404, 410
 Piccioli, 407
 Pierce, 407
 Pincherle, 409
 Prompt, 406
 Proth, (398)

 Ranum, 410
 Réalis, 404

 Riccati, 407
 Ruggieri, 405

 Sancery, (397)
 Scheibner, 408
 Scherk, 411
 Schlegel, 411
 Schönflies, 403
 Seliwanov, 403
 Serret, 394
 Siebeck, 394
 Simson, 393
 Stirling, 407
 Study, 409
 Svanberg, 411
 Sylvester, 401, 403, 411

 Tagiuri, 404
 Tarn, 411
 Traverso, 410

 Valroff, 405
 Vész, 411
 Vogt, 411
 Von Sterneck, (398)

 Wasteels, 405
 Weiss, 411
 White, 405
 Whitworth, 411

 Zeuthen, 405

CH. XVIII. THEORY OF PRIME NUMBERS.

- Andreoli, 434
 Aubry, 422
 Auric, 414

 Bachmann, 416, 418, 432
 Bang, 418-9
 Baranowski, 432
 Barinaga, 428, 438
 Bauer, 419, 420
 Berton, 416
 Bertrand, 435 (413, 425, 436)
 Bervi, 419
 Biddle, (426)
 Bindoni, 427
 Birkhoff, 418
 Boije af Gennäs, 414
 Bonolis, 436
 Bougaief, 422, 429 (430-1)
 Bouniakowsky, 421
 Braun, 414, 421, 437
 Brocard, 425-6, 436
 Brun, 438

 Cahen, 414, 419, 436

 Cantor, 422, 425
 Carmichael, 420, 428
 Catalan, 421, 429, 431, 435 (426)
 Cesàro, 430 (432, 435)
 Chabert, 420
 Chiari, 428
 Cipolla, (426)
 Coblyn, 438
 Cole, (426)
 Cunningham, 417, 423
 Curjel, 429, 431-2

 Dedekind, 415
 De Jonquières, 429 (432)
 De la Vallée Poussin, 416, 418, 439-440 (417)
 De Mondésir, 430
 De Montferrier, 426
 De Polignac, A., 424, 439 (425)
 De Polignac, C., 436-7
 De Rocquigny, 425
 Desboves, 415, 422, 435 (436)

 Descartes, 421
 Deschamps, 439
 Devignot, 426
 Dickson, 417
 Dirichlet, 415, 417 (416, 418)
 Dormoy, 437
 Dupré, 415
 Durand, 415

 Eneström, [421]
 Eratosthenes, (424)
 Escott, 420, 426, 428
 Euclid, 413
 Euler, 413, 415, 420-1, 424, 426

 Fontebasso, 427
 Frobenius, 421

 Gambioli, 427
 Gauss, 438
 Gegenbauer, 413, 427, 431-3 (426, 435)
 Genocchi, 418

- Genty, (426)
 Giovannelli, 424
 Goldbach, 420-1, 424
 Graefe, 432
 Gram, 430
 Guibert, 425

 Hacks, 414, 427
 Hadamard, 424, 439, 440
 Hammond, 423, 429, 438
 Hardy, 438, 440
 Hargreave, 429
 Haussner, 422 (423)
 Hayashi, 433
 Heiberg, [413]
 Heine, 415
 Hensel, 416, 418-9
 Hermite, 437
 Hoffmann, 430
 Hossfeld, 431
 Hurwitz, (426)

 Isenkrahe, 437
 Iwanow, 419, 437

 Jaensch, 413
 Johnsen, 429
 Jolivald, 427 (426)

 Klein, 438
 Kössler, 435
 Kraft, 426
 Kraus, 418
 Kronecker, 413, 416, 418,
 425, 429 (414)
 Kummer, 413

 Labey, [413]
 Lagrange, 424-5 (426)
 Lambert, (426)
 Landau, 417-9, 423, 425,
 435-8, 440
 Landry, 418
 Laurent, 427 (433)
 Lebesgue, 418-9 (426)
 Lefébure, 418

 Legendre, 415, 420, 429, (416,
 430-1, 434-5)
 Leibniz, (426)
 Le Lasseur, 420
 Lemaire, 420, 426
 Lemoine, 424
 Le Vavas seur, 437
 Levi-Civita, 433
 Lévy, 414, 421
 Lionnet, 422, 426, 429 (423)
 Lipschitz, 429 (432)
 Littlewood, 440
 Lorenz, 430
 Lucas, 418-9, 421 (426, 428)
 Lugli, 431

 Maillet, 423, 425, 436
 Märcker, 436
 Markow, 437
 Martin, 426
 Mathews, 429
 Mathieu, 425
 Meissel, 429, 431 (432)
 Meissner, 427, 438
 Merlin, 424
 Mertens 416-8
 Métrod, 415
 Meyer, 418
 Minetola, 427, 434
 Minin, 433
 Miot, 421
 Moreau, 416

 Oltramare, 420
 Oppermann, 435

 Paci, 430
 Pascal, 420
 Perott, 413-4
 Petrovitch, 434
 Pexider, 433
 Piltz, 416
 Pocklington, 419, 428
 Proth, 435

 Rados, 428
 Riemann, 439

 Ripert, 423, 425
 Rogel, 429, 431, 433-4

 Sardi, (426)
 Schaffgotsch, (426)
 Scheffler, 416, 431
 Schepp, [420]
 Schering, 418
 Scherk, 436
 Schur, 419
 Serret, 418-9, 435
 Smith, 436, 439
 Speckmann, 416
 Stäckel, 423 (422)
 Stasi, 428
 Stern, 424, 426
 Stieltjes, 414, 436
 Störmer, 437 (414)
 Studnička, 423
 Sylvester, 416, 418-9, 422-3,
 429, 431-2, 435, 437, 439
 (433)
 Tchebychef, 413, 435, 437,
 439 (426)
 Teege, 417
 Terquem, 421, 436
 Thue, 414
 Torelli, 440

 Vahlen, 419
 Van der Corput, 419
 Vandiver, 418
 Van Laar, 431
 Vecchi, 424, 428
 Von Koch, 427, 432 (433)
 Von Sterneck, 419, 427, 435

 Waring, 421, 425
 Weber, 417-8
 Wendt, 418
 Wertheim, 429
 Wigert, 432 (428, 434)

 Zignago, 416
 Zondadari, 428
 Zsigmondy, 418, 427 (426)

CH. XIX. INVERSION OF FUNCTIONS; MÖBIUS' FUNCTION $\mu(n)$; NUMERICAL INTEGRALS AND DERIVATIVES.

- Axer, 449

 Bachmann, 445-6, 449
 Baker, 443
 Berger, 444, 446 (443)
 Bervi, 451
 Borel and Drach, 449
 Bougaïef (Bugaïev), 442-3,
 449-451 (448)
 Cahen, 449

 Cesàro, 443, 450
 Cistiakov, 451

 Dedekind, 441-2 (444, 446)
 Dirichlet, (445)

 Elliott, 447

 Fatou, 448
 Fleck, 448
 Furlan, 448

 Gegenbauer, 447, 450 (443)
 Glaisher, (441)

 Hackel, 448

 Kluyver, 448
 Knopp, (448)
 Kronecker, 447 (443, 448)
 Kusnetzov, 448

 Laguerre, 442

- Landau, 448-9
 Lémeray, 447
 Liouville, 441-2
 Lipschitz, 445
 Lucas, 445
 Meissel, 441
 Meissner, 448
 Merry, 442 (444)
- Mertens, 442, 446 (448)
 Möbius, 441 (443)
- Nazimov, (448)
- Seliwanov, 446
 Shelly, 451
 Steffensen, 449
- Stieltjes, 449
- Tschistiakow, 451
- Von Koch, 446
 Von Sterneck, 444-6 (442, 448)
- Zsigmondy, 444-5.

CH. XX. PROPERTIES OF THE DIGITS OF NUMBERS.

- Agronomof, 464
 Aiyar, 458
 Andreini, 459, 461
 Andreoli, 464
 Anonymous, 454, 458
- Barbier, 457
 Barillari, 455
 Barisien, 462
 Barlow, 453
 Berdellé, 457
 Bertrand, 455
 Bianchi, 455
 Biddle, 463
 Booth, 455
 Boutin, 461
 Bouton, 460
 Brocard, 464
 Brownell, 453
 Burg, 464
- Calvitti, 461
 Cantor, 455 (458)
 Catalan, 456
 Cattaneo, 463
 Cesàro, 457 (461)
 Crelle, 454 (456)
 Cunningham, 458, 460, 462-4
- Davey, 454
 De Rocquigny, 457
 De Sanctis, 459, 464
 Dickson, 460
 D'Ocagne, 457
 Drot, 455
- Emsmann, 455
 Escott, 458, 462
- Flood, 455
- Fourrey, 465
 Français, 454
- Gegenbauer, 458
 Gelin, 465
 Gérardin, 461-2
 Gergonne, 454
 Glaisher, 456
 Goormaghtigh, 464
 Grunert, 455
- Halliday, 465
 Hauke, 459
 Hayashi, 459
 Hill, 453
 Hoskins, 456
- Ingleby, 455
- Jänichen, 462
 Johnson, 458
- Kessler, 457
 Koppe, 461
 Kraitichik, 458
 Kraus, 458
- Laisant, 456-8 (454)
 Lemoine, 457, 464
 Lewis, 463
 Lucas, 458, 465
- Mackay, 457
 Maillet, 464
 Malo, 461
 Mansion, 456
 Martin, 456
 Metcalfe, 460
 Moore, 460
 Morel, 456
- Moret-Blanc, 457
 Moulton, 465
- Nannei, 462
- Osana, 465
 O'Shaughnessy, 465
- Palmstrom, 458-9 (461)
 Perkins, 456
 Piccioli, 460
 Plateau, 456 (460, 463)
- Rutherford, 455
- Saint, 453 (456)
 Sampson, 455
 Sebban, 464
 Simmons, 457
 Stasi, 463
 Storr, 458
 Strauss, 458
 Suchanek, (459)
 Szegö, 462
- Tagiuri, 460
 Tanner, 456
 Tédénat, 454
 Teilhet, 460
 Thié, 463
- Valentin, 459
 Vercellin, 462
 Von Schrutka, 464
- Welsch, 464
 Wertheim, 459
 White, 465
 Wiggins, 460
 Witting, 462
- Zühlke, 461

SUBJECT INDEX.

Abundant, 3, 7, 11, 14, 15, 20, 31-3
 Agreeable, 38, 458
 Algebraic numbers, 86, 221, 245, 251, 322, 379, 417, 447-8
 Aliquot parts, 3, 50-8
 Amantes, 39
 Amiable, 38, 41
 Amicable, 5, 38-50
 ——— of higher order, 49, 50
 ——— triple, 50
 Anatomiae numerorum, 348
 Approximation, 114-5, 158, 281-3, 318, 330-1, 352, 354, 411, 422-3, 430, 448 (see asymptotic, mean)
 Arrangement in cycles, 269
 Arithmetical progression, 100-1, 114, 131, 336, (see prime)
 Associated numbers, 64-6, 73
 Asymptotic, 119, 122, 126-7, 129-132, 134-6, 138, 144, 154-5, 214-5, 289, 291, 294, 301-2, 305-6, 308, 317-325, 328, 333, 416-9, 434-6, 438-440, 450 (see approximation, mean)
 Aurifeuillian, 386, 390
 Base, 178, 182, 186, 199, 273, 338, 340-1, 354-5, 369, 373, 375, 379, 385, 398, 454, 456, 458-460, 463-4 (see digits, periodic)
 Befreundete, 38
 Belongs (see exponent)
 Bernoullian numbers, 100, 109, 110, 112, 140-1, 145-6, 220, 274, 278, 309, 311
 Bernoulli's function, 268, 325
 Bertrand's postulate, 132, 413, 425, 435-6
 Bilinear form, 409
 Binomial coefficients, 59, 62, 67, 77, 91, 97, 99, 266-278
 ——— congruence, 92-5, 105, 175, 177, 204-222, 388, 391
 ——— ———, identical, 78, 82, 87-9, 94-5
 Casting out nines, 337-346
 Characters, 201, 415
 Circular permutations, 75, 78, 81, 131, 136

(484)

Combinations, 77, 90-1, 106, 261, 281, 303, 410
 Complementary fractions, 156
 Congeneres, 39
 Congruence (see binomial)
 ———, cubic, 252-6, 262
 ———, higher, 223-61
 ———, identical, 73, 87-9
 ———, involving factorials, 275-8, 428
 ———, irreducible, 84, 234-52
 ———, quartic, 254-5, 259, 260
 Congruent form, 362
 ——— fractions, 258-9
 ——— series, 259
 Conjugate functions, 444
 Consecutive numbers, 147, 332, 353, 355, 373, 457 (see product)
 Continued fractions, 138, 158, 210, 363, 367-8, 381, 393, 399, 403, 408-9
 Crib (see sieve)
 Criteria for given divisor, 337
 Cyclotomic function, 199, 245, 378, 383-5, 387-90, 418
 Decimal (see periodic)
 Defective, 3
 Deficient, 3
 Determinant, 77, 87, 97, 137, 149, 150-1, 226, 228, 231, 233, 261, 288, 295, 321, 336, 368, 399, 410-1, 444, 446
 ——— $\equiv c \pmod{m}$, 155, 261
 ——— of Smith, 122-4, 127-130, 136
 Diatomic series, 439
 Differences of order m , 62-4, 74, 78, 79, 204
 ——— ——— two primes, 424-5
 ——— ——— ——— squares, 357
 Digits, 81, 343, 353-4, 358, 360, 366, 438, 453-65
 ——— of perfect number, 7, 10, 17, 20
 ——— permuted in multiples, 164-5, 170, 174, 176-7, 458-9

Digits, sum of, 263-4, 266, 272, 337-8, 342-3, 367, 455, 457-8, 461-4
 Diminute, 3, 4
 Equivalent fractions, 135
 Euclidean number, 28
 Euler's constant, 122, 134, 136, 281-3, 289, 294, 317-24, 328-30
 ——— criterion, 67, 205
 ——— generalization of Fermat's theorem, 60-89, 398, 400
 ——— numbers, 363
 ——— ϕ -function, 82, 85, 110, 113-58, 182, 285-6, 293, 312, 333-6, 404, 434, 441-2, 446
 ——— ——— ———, generalized by Schemmel, 147
 ——— ——— ——— ——— Jordan, 123, 132, 147, 252, 298-9
 Excédant, 3
 Excess E of divisors $4m+1$ over divisors $4m+3$, 281, 289, 293, 295-6, 300-1, 308, 318-9
 ——— of odd over even divisors, 290-1, 317-8
 Exclusion method, 207, 369-70
 Exponent, 61, 112, 163, 169, 181-204, 240, 242-3, 246, 257, 259, 260 (see Haupt)
 ——— to which 10 belongs, 159-204, 339, 341-2
 ——— ——— ——— 2 belongs, 111, 181, 190-1, 193, 198, 200, 203, 369-70
 Factor tables, 347 (see graphical)
 Factorial, 62-3, 77, 263-78
 Factoring, 13, 25, 241, 248, 252, 357 (see graphical, criteria, sieve)
 ———, number of ways of, 52, 109, 282, 285, 298, 331
 Factors of $10^n \pm 1$, 159-179
 ——— ——— $2^n - 1$ (see perfect)
 ——— ——— $a^n \pm b^n$, 258, 381-91

- Farey series, 155-8
 Fermatian function, 385
 Fermat's numbers $2^n + 1$, 94,
 140, 199, 375, 398, 401
 ——— theorem, 12, 17, 18,
 59-89, 179
 ———, converse of,
 91-5
 ———, generaliza-
 tion, 84-9, 406 (see Galois)
 Finite algebra, 388
 ——— differences, 250, 394,
 407
 ——— field, 247, 250
 Flächen Zahlen, 4
 Frequency of a divisor, 126

 Galois field, 232, 247, 250
 ——— imaginary, 233-55
 Galois' generalization of Fer-
 mat's theorem, 235, 240,
 246-7, 249, 250, 252, 403
 ——— Wil-
 son's theorem, 240, 246-7,
 252
 Gaussien, 194
 Graphical factoring, 351, 353-
 4, 356, 365, 369, 372, 374
 ——— representation of di-
 visors, 330, 351, 354
 Greatest common divisor,
 139, 147, 150, 252, 328,
 332-6, 394, 401-3, 447,
 456, 462 (see determinat
 of Smith)
 ——— divisor, 329, 331
 ——— integer in, 89, 119,
 121-2, 126, 130, 132, 138,
 144, 153, 158, 263, 282,
 293, 295, 297-9, 302-3,
 319, 427, 429-432, 450-1
 Goldbach's theorem and anal-
 ogues, 421-5
 Golden section, 411
 Ground forms, 268
 Groups, 78, 80-1, 84-5, 131,
 137, 152, 155, 177, 194,
 196-8, 201, 203, 216, 221,
 248, 251, 268, 287, 332,
 356, 414-5
 Haupt-exponent, 190, 200, 203
 Hexagon, 9, 411
 Highest prime power in $m!$,
 263, 272
 ——— a poly-
 nomial, 334
 Highly composite number, 323
 History, 32, 84, 157, 200,
 342, 353
 Hyper-even number, 379

 Hyper-exponential number,
 379

 Idoneal (idoneus), 361-5
 Imperfectly amicable, 50
 Index, 85, 182-3, 185, 188,
 190-4, 197-204, 211, 240,
 244-5, 249, 251
 Indian, 337
 Indicator, 118, 131, 155, 186,
 194, 200
 Indivisibilis, 6
 Integral logarithm, 353, 417,
 440
 Invariant, 89, 232-3, 260, 364
 Inversion, 84, 120, 127, 129,
 132-3, 135, 140, 145, 150,
 153, 234, 296, 429, 430,
 441-8
 Irreducible function, 234-252
 ——— fraction, 126, 129,
 133, 138, 155-8, 162, 175

 Kerne, 334
 Körper Zahlen, 4
 Kronecker's plane, 155

 Lattice, 173
 Leaf arrangement, 411
 Least common multiple, 82,
 328, 332-6, 445, 464
 ——— residue, 341-2, 344, 369
 Legendre-Jacobi symbol, 109,
 210, 219, 249, 251, 255, 260,
 276, 288, 300, 308, 330, 364,
 382, 385, 394, 398
 Linear differential form, 248,
 250
 ——— forms of divisors, 160,
 362-4, 370, 382, 386, 390,
 399
 ——— function, 117-8, 134,
 204-5
 ——— numbers, 4
 Lucas' u_n, v_n , 218, 395, 418
 Lucassian, 27

 Mangelhaft, 3
 Matrix, 137, 226, 228, 233
 Maximum divisor, 332
 Mean, 281, 291-4, 301-2, 305,
 312, 318, 320, 328-331, 333,
 335, 447 (see asymptotic)
 Mediation, 156
 Mersenne number, 31
 Möbius' (Merten's) function
 $\mu(n)$, 86, 122, 127-9, 144-5,
 148-9, 150-1, 265, 289, 322-
 3, 329, 335, 431, 441-9, 462
 ——— gener-
 alized, 135-6

 Modular system, 88, 249,
 251, 402
 Mosaic, 212
 Multinomial coefficient, 59,
 266-78
 Multiply perfect, 33

 Nim (game), 460
 Nombres associés, 50
 Norm, 236, 252, 322
 Normal order, 325
 Number of divisors, 51, 54,
 135-6, 142, 279-325, 328,
 443, 451
 ——— integers divis-
 ible by n th power, 327-32
 ——— solutions of
 $u_1 \dots u_k = n$, 125, 149, 291,
 298, 308, 312, 317, 324
 ——— $n = x^a y^b$,
 318
 Numerical integrals and de-
 rivatives, 152, 449

 Order modulo m , 138
 ——— of root, 189

 Partial fraction, 73, 135, 161,
 198, 410
 Partition, 279, 290, 292, 303,
 312, 427, 438
 Patrone, 349
 Pedal triangle, 86, 388, 402
 Pell equation, 56, 367-8, 393
 Pentagonal number, 279, 292,
 312
 Perfect number, 3-33, 38
 ——— of second kind,
 58
 Period, 133, 182, 202, 207
 Periodic fraction, 75-6, 82,
 92, 159-179, 193, 202, 339-
 341, 371, 379, 386, 454
 Permutations, 78-80, 131, 136
 Plateau's theorem, 456, 460,
 463
 Pluperfect, 33
 Plus quam-perfectus, 3
 Polygon, curvilinear, 85
 ———, inscribed in cubic
 curve, 85, 150
 ———, regular, 71, 75, 133,
 139, 193, 375
 Polynomial, divisors of, 384,
 393-4
 ——— in x divisible by m for
 every x , 87, 89, 336
 Primary function, 240
 Prime functions (see irredu-
 cible)
 ——— pairs, 353, 425, 438

- Primes $6n \pm 1$, 7 (see difference, highest)
 —, asymptotic distribution of, 439, 449
 —, density of, 329, 416
 — in arith. progression, 425
 —, infinity of, 413
 — — — — — in arith. progressions, 85, 395, 415–20, 436
 —, large, 352–4, 362, 365, 386, 388
 —, law of apparition of, 396, 398, 406
 — — — — — repetition of, 396–8
 —, miscellaneous results on, 436–9
 —, number of, 352–4, 429–35, 450
 —, product of, 126
 — represented by quadratic forms, 417
 — — — — — polynomials, 333, 414, 418, 420–1
 —, sum of two, 421–4, 435
 Primes, tables of, 347, 381
 —, test for, 35, 276, 302, 305, 360–65, 370, 374, 376–8, 380, 396–404, 426–8, 445
 —, to base 2, 22, 353–4
 Primitive divisor of $a^n - b^n$, 388
 — λ -root, 202
 — non-deficient number, 31
 — number, 327, 334
 — root, 63, 65, 72, 103, 117, 181–204, 222, 378–9
 — — — — —, imaginary, 235–252
 — — — — — of unity, 133, 136
 Probability, 138, 302, 308, 328, 330, 333, 335, 407, 438
 Product of consecutive integers, 79, 263–4, 269, 331
 — — — — — differences, 269
 — — — — — divisors, 58, 332
 Pronic, 357
 Quadratic forms, 109, 130, 158, 207, 210, 219, 276, 318, 330, 361–5, 369–70, 400, 415–8, 420–1
 — — — — — residues, 23, 25, 29, 65–8, 71, 76, 92, 109, 165, 185, 189, 190, 196–8, 202, 210, 213–4, 218, 221, 231, 240, 245–6, 253–5, 275, 277, 360, 363, 365, 373, 382, 393, 395–6, 403
 Quasi-Mersenne number, 390
 Quotient $(\alpha_{\phi, m}) - 1/m$, 102, 105–112
 — — — — — $\{(p-1)! + 1\}/p$, 109, 112
 Rank (see matrix)
 Recurring series, 376–7, 393–411
 — — — — —, algebraic theory of, 407
 Reducible law of recurrence, 409–10
 Redundantem, 3, 4
 Remainders on dividing n by $1, \dots, n$, 290, 313, 327–31
 Roots of unity, 133, 136, 183–4, 245, 250, 256, 419
 Secondary number, 327
 — — — — — root, 191
 Series of composition, 332
 — — — — — Lamé, 411
 — — — — — Leonardo Pisano, 393
 Sieve of Eratosthenes, 8, 347–8, 353–6, 424, 439
 Similar modulo k , 260
 Simple system of numbers, 455, 458
 Solution of alg. equations, 407–8
 Sous-double, 33
 Squares, 52, 54, 284–6, 358, 361, 366, 453–464
 Stencil, 349, 356, 359
 Substitutions, 75, 78–80, 82, 85, 158, 232, 262
 Sum of divisors, 5, 18, 19, 22, 42, 48, 52–8, 135, 139, 279–325, 445, 450
 — — — — — k th powers of divisors, 38, 123, 151, 286–325, 450
 — — — — — — — — integers $< n$, 95, 106, 121, 123, 126, 140, 332
 — — — — — four squares, 283
 — — — — — two squares, 247, 286, 340, 360, 381–2, 390, 402–3
 Superfluos, 3, 4
 Symbolic, 99, 119, 124, 141–2, 144–5, 148, 248, 250, 278, 296, 395, 399, 402, 449
 Symbols, $E(n)$, 281; $E_r(n)$, 296; $F(a, N)$, 84; F_r , 375; $H(m)$, H_m , 264; $J_k(n)$, 147; M_q , 31; $\mu(n)$, 441; O , 305; P_m , 33; $\phi(n)$, 61, 113; $\phi_k(n)$, 140; q_u , 105, 109; $s^k(n)$, 48; s_n , 95; S_n, m , 96; $\sigma(n)$, 53, 279, 446; $\sigma_k(n)$, $\tau(n)$, $T(n)$, 279; $T_k(n)$, 291; $\theta(n)$, 429; U_n, u_n , 393; $\zeta(s)$, 292; $[x]$, 115, 276; $/n$, 42; *before author, not available.
 Symmetric functions mod. p , 70, 95, 106, 143
 — — — — — number, 112, 455, 463–4
 Tables, 10, 14, 16, 18, 21–2, 25, 27, 30–2, 37–8, 45, 48–9, 54–5, 110–2, 126, 135, 137, 140, 156–7, 160–79, 181, 183, 185, 187–203, 213, 217, 219, 222, 244–5, 248–51, 254, 262, 296, 308, 318, 331, 339–41, 347–58, 361–4, 366–7, 379, 381–4, 386, 388, 390–1, 399, 417, 422, 432, 446, 457
 Talmud, 337
 Totient, 124–5, 148, 153, 246
 — — — — — point, 154
 Totitives, 98, 124, 130–1, 246
 — — — — — all primes, 132, 134
 Triangular number, 7, 9, 20, 59, 284, 290, 295, 302, 310, 373, 425, 427
 Trinomials, factors of, 391
 Überflüssig, 3
 Überschliessende, 3
 Übervollständig, 3
 Unvollkommen, 3
 Unvollständig, 3
 Verwandte, 38, 47
 Vollkommen, 3
 Vollständig, 3
 Wilson's theorem, 59–91, 99, 103, 275
 — — — — —, converse of, 63, 427–8
 — — — — —, generalization of, 65, 68–74, 77–84, 87, 90–1 (see Galois)
 Zeta function, 121, 125–7, 134, 139, 149, 292–3, 298–9, 310, 318, 322, 324, 328, 331, 439, 448

- Primes $6n \pm 1$, 7 (see difference, highest)
 —, asymptotic distribution of, 439, 449
 —, density of, 329, 416
 — in arith. progression, 425
 —, infinity of, 413
 — — — — — in arith. progressions, 85, 395, 415–20, 436
 —, large, 352–4, 362, 365, 386, 388
 —, law of apparition of, 396, 398, 406
 — — — — — repetition of, 396–8
 —, miscellaneous results on, 436–9
 —, number of, 352–4, 429–35, 450
 —, product of, 126
 — represented by quadratic forms, 417
 — — — — — polynomials, 333, 414, 418, 420–1
 —, sum of two, 421–4, 435
 Primes, tables of, 347, 381
 —, test for, 35, 276, 302, 305, 360–65, 370, 374, 376–8, 380, 396–404, 426–8, 445
 —, to base 2, 22, 353–4
 Primitive divisor of $a^n - b^n$, 388
 — λ -root, 202
 — non-deficient number, 31
 — number, 327, 334
 — root, 63, 65, 72, 103, 117, 181–204, 222, 378–9
 —, imaginary, 235–252
 — of unity, 133, 136
 Probability, 138, 302, 308, 328, 330, 333, 335, 407, 438
 Product of consecutive integers, 79, 263–4, 269, 331
 — differences, 269
 — divisors, 58, 332
 Pronic, 357
 Quadratic forms, 109, 130, 158, 207, 210, 219, 276, 318, 330, 361–5, 369–70, 400, 415–8, 420–1
 — residues, 23, 25, 29, 65–8, 71, 76, 92, 109, 165, 185, 189, 190, 196–8, 202, 210, 213–4, 218, 221, 231, 240, 245–6, 253–5, 275, 277, 360, 363, 365, 373, 382, 393, 395–6, 403
 Quasi-Mersenne number, 390
 Quotient $(a\phi^m - 1)/m$, 102, 105–112
 — $\{(p-1)! + 1\}/p$, 109, 112
 Rank (see matrix)
 Recurring series, 376–7, 393–411
 —, algebraic theory of, 407
 Reducible law of recurrence, 409–10
 Redundantem, 3, 4
 Remainders on dividing n by $1, \dots, n$, 290, 313, 327–31
 Roots of unity, 133, 136, 183–4, 245, 250, 256, 419
 Secondary number, 327
 — root, 191
 Series of composition, 332
 — Lamé, 411
 — Léon, 393
 Sieve of Eratosthenes, 347–8, 353–6, 424,
 Similar modulo k , 260
 Simple system of r , 455, 458
 Solution of alg. eq., 407–8
 Sous-double, 33
 Squares, 52, 54, 284, 361, 366, 453–464
 Stencil, 349, 356, 358
 Substitutions, 75, 78–80, 82, 85, 158, 232, 262
 Sum of divisors, 5, 18, 19, 22, 42, 48, 52–8, 135, 139, 279–325, 445, 450
 — k th powers of divisors, 38, 123, 151, 286–325, 450
 — — — — — integers $< n$, 95, 106, 121, 123, 126, 140, 332
 — — — — — four squares, 283
 — — — — — two squares, 247, 286, 340, 360, 381–2, 390, 402–3
 Superfluos, 3, 4
 Symbolic, 99, 119, 124, 141–2, 144–5, 148, 248, 250, 278, 296, 395, 399, 402, 449
 Symbols, $E(n)$, 281; $E_r(n)$, 296; $F(a, N)$, 84; F_r , 375; $H(m)$, H_m , 264; $J_k(n)$, 147; M_q , 31; $\mu(n)$, 441; O , 305; P_m , 33; $\phi(n)$, 61, 113; $\phi_k(n)$, 140; q_u , 105, 109; $s^k(n)$, 48; s_n , 95; $S_{n,m}$, 96; $\sigma(n)$, 53, 279, 446; $\sigma_k(n)$, $\tau(n)$, $T(n)$, 279; $T_k(n)$, 291; $\theta(n)$, 429; U_n , u_n , 393; $\zeta(s)$, 292; $[x]$, 115, 276; f_n , 42; *before author, not available.
 Symmetric functions mod. p , 70, 95, 106, 143
 — number, 112, 455, 463–4
 Tables, 10, 14, 16, 18, 21–2, 25, 27, 30–2, 37–8, 45, 48–9, 54–5, 110–2, 126, 135, 137, 140, 156–7, 160–79, 181, 183, 185, 187–203, 213, 217, 219, 222, 244–5, 248–51, 254, 262, 296, 308, 318, 331, 339–41, 347–58, 361–4, 366–7, 379, 381–4, 386, 388, 390–1, 399, 417, 422, 432
 Job 8463. Date.....
 Mend by..... Time.....
 Stab by..... No. Sect..... Sew by.....
 Score..... Press..... Strip Sect.....
 This book bound by Pacific Library Binding Company, Los Angeles, specialists in Library Binding. Our work and materials are guaranteed to wear indefinitely to satisfaction of purchaser, and any defects appearing in either will be made good without additional charge. "Bound to wear."
 Ubervollständig, 3
 Unvollkommen, 3
 Unvollständig, 3
 Verwandte, 38, 47
 Vollkommen, 3
 Vollständig, 3
 Wilson's theorem, 59–91, 99, 103, 275
 —, converse of, 63, 427–8
 —, generalization of, 65, 68–74, 77–84, 87, 90–1 (see Galois)
 Zeta function, 121, 125–7, 134, 139, 149, 292–3, 298–9, 310, 318, 322, 324, 328, 331, 439, 448

SAVED

1

7

8

10X

SCIENCES 21

UC SOUTHERN REGIONAL LIBRARY FACILITY



D 000 378 498 0

Engineering &
Mathematical
Sciences
Library

QA

241

D56A

V.1

COPY 2

LIBRARY BRANCH,
UNIVERSITY OF CALIFORNIA,
LIBRARY,
LOS ANGELES, CALIF.

LIBRARY

JUL 72

STACK

JUN 28 1982

ANNEX

REC APR 26

APR 25 1982

RECEIVED

APR 27 1982

STACK ANNEX

RECEIVED

NOV 27 1984

STACK ANNEX

STACK

APR 04 1988

ANNEX

RECEIVED

JAN 14 1988

STACK ANNEX

UC SOUTHERN REGIONAL LIBRARY FACILITY



D 000 378 498 0

Engineering &
Mathematical
Sciences
Library

QA

241

D56h

v.1

Cop. 2

SOUTHERN BRANCH,
UNIVERSITY OF CALIFORNIA,
LIBRARY, JUL 72
LOS ANGELES, CALIF.

University of California
SOUTHERN REGIONAL LIBRARY FACILITY
405 Hilgard Avenue, Los Angeles, CA 90024-1388
Return this material to the library
from which it was borrowed.

PAS - QL

OCT 05 1992

PAS - QL

JAN 19 1993

APR 19 1993

~~REC'D~~ PAS APR 19 1993

10/16/95

REC'D C.L. SEP 25 '95

REC'D LD-URL
WK 2 MAY 07 1997
APR 23 1997

LD-URL
WK 2 OCT 11 1997

OCT 16 2006

ED

1988

ANNEX

UC SOUTHERN REGIONAL LIBRARY FACILITY



D 000 378 498 0

Engineering &
Mathematical
Sciences
Library

QA
241
D56h
v.1
Cop. 2

SOUTHERN BRANCH,
UNIVERSITY OF CALIFORNIA,
LIBRARY,
LOS ANGELES, CALIF.

LIBRARY
JUL 72

California
Regional
Library